

# NetFlow Analyzer

Professional and Professional Plus Edition

## Bandwidth Monitoring & Traffic Analysis - User Guide

## Table Of Contents

<b>INTRODUCTION.....</b>	<b>4</b>
What's New in this Release? .....	5
<b>INSTALLATION AND SETUP .....</b>	<b>9</b>
System Requirements .....	9
Prerequisites.....	11
Installing and Uninstalling.....	12
Starting and Shutting Down.....	13
Accessing the Web Client.....	15
License Information .....	16
<b>CONFIGURING FLOW EXPORTS .....</b>	<b>17</b>
Cisco Devices (NetFlow) .....	18
Configuring Cisco Devices.....	18
Cisco® NetFlow Device Support .....	19
Configuring Cisco ASA 5500 series.....	21
Configuring NetFlow Export on an IOS Device .....	22
Configuring NDE on Catalyst 6000 Series Switches.....	24
Configuring NDE on a Native IOS Device .....	25
Configuring NDE on 4000 Series Switches .....	26
Configuring NetFlow for BGP .....	27
Juniper Devices (cflowd/J-Flow).....	29
Configuring flow exports on Juniper Routers.....	29
Huawei/3com devices(Netstream).....	30
Configuring NetStream Export.....	30
Nortel Devices(IPFIX).....	31
Configuring IPFIX Export .....	31
sFlow exporting devices .....	32
sFlow Supported Devices .....	33
Enabling sFlow.....	35

<b>GETTING STARTED .....</b>	<b>37</b>
Dashboard view .....	38
Dashboard view .....	40
Dashboard Interface View .....	41
Dashboard AS View.....	46
Google Map View .....	47
IP Groups View.....	48
<b>TRAFFIC REPORTS.....</b>	<b>49</b>
Real-time Traffic Graphs.....	50
Top Applications .....	52
Top Hosts .....	54
QoS.....	55
Top Conversations.....	57
AS Traffic Reports .....	58
Troubleshooting.....	59
Consolidated Reports .....	60
Compare Report - NetFlow Analyzer Global Report.....	61
Search Report.....	62
<b>ADMIN OPERATIONS.....</b>	<b>63</b>
Product Settings .....	64
Advanced Settings.....	65
Storage Settings .....	67
Mail Server / Proxy Server Settings.....	68
Google Map Settings .....	69
Application Mapping, Application Group, DSCP Mapping and DSCP Group .....	70
IP Group Management .....	74
Alert Profiles Management .....	78
Schedule Reports .....	81
Device Group Management.....	86
Billing.....	88

NBAR.....	93
NBAR Report .....	96
NBAR Supported Applications.....	97
NBAR supported platforms & IOS Versions .....	100
Flexible NetFlow and NBAR integration .....	101
CBQoS.....	103
CBQoS Child Policies .....	111
User Management .....	114
License Management .....	116
Change Password .....	118
<b>NETFLOW ANALYZER ADD-ON.....</b>	<b>119</b>
VoIP Monitor .....	120
Adding a New VoIP Monitor.....	121
Configuring call settings and threshold template .....	123
Viewing Top 10 Call Paths.....	124
FAQs on VoIP Monitor .....	125
<b>CONTACTING TECHNICAL SUPPORT .....</b>	<b>127</b>
<b>FREQUENTLY ASKED QUESTIONS .....</b>	<b>128</b>
<b>OTHER CONFIGURATIONS .....</b>	<b>139</b>
Configuring MSSQL database .....	139
Migrating NetFlow Analyzer Data from MySQL to MSSQL Database .....	139
<b>APPENDIX.....</b>	<b>141</b>
Working with SSL .....	142
SNMP Trap Forwarding .....	144
Database Backup .....	145
Configuration Backup .....	146
Aggregated Data Backup.....	147
Geo Locations.....	148

## Introduction

---

ManageEngine NetFlow Analyzer is a web-based bandwidth monitoring tool that performs in-depth traffic analysis using data exported from **NetFlow / Netstream / cflowd / J-Flow / sFlow / IPFIX** flows.

This data provides granular details about network traffic that has passed through an interface. NetFlow Analyzer processes this information to show you what applications are using bandwidth, who is using them, and when. Extensive graphs and reports make this information easy to analyze, and also help accelerate the troubleshooting process.

This User Guide will help you install NetFlow Analyzer, and get familiar with the user interface. If you are unable to find the information you are looking for in this document, please let us know at [netflowanalyzer-support@manageengine.com](mailto:netflowanalyzer-support@manageengine.com)

## What's New in this Release?

### New Features in Release 8.0

The latest release of NetFlow Analyzer (**8.0**) can be downloaded from the website at <http://www.netflowanalyzer.com/download.html>

Feature	Description
IPSLA (VoIP)	Monitors the key performance metrics of the VoIP network to determine its health. The parameters measured include Jitter, Latency, Packet Loss etc.
SNMP V3 support	Support for SNMP V3 has been added in this build
FNF - NBAR integration	Now users can get data on NBAR by configuring flexible NetFlow
V9 Sampling	NetFlow Analyzer now does NetFlow V9 sampling as well
Cisco ASA	NetFlow Analyzer now supports Cisco ASA (ISO version 8.2 onwards)
CBQoS Child Policy	Child policies can be created under parent policies
PDF Option in CBQoS	CBQoS reports can be exported as PDF
Geo Locations reports of IP Addresses	Resolves and groups IP addresses into groups of countries. Lists the traffic usage and bandwidth utilization of the link by the IP address from separate countries
Single Click Scheduling Option	Scheduling reports have been made easier now
Network Layout using google maps and Google map widgets	Devices can be located on google maps and a click on link between devices will give details about the link utilization and more
More Graphical Widgets and some new Widgets added in Dashboard	The widgets have become more graphical, which means it is now easier to interpret data
Sampling rate accounted during the flow calculation	Flow calculation also takes sampling rate(defined by the network administrator) into account
Global search for IP Address link	Type in the IP address of the source / destination / network... or any of the given choices and Voila! you will get Traffic IN and Traffic OUT details for the particular IP address
Operator specific Dashboard permissions	Operators and guest accounts can also create dashboards
Top N AS reports	Top N AS reports can be selected from the drop down
Last 15, 30 Min reports	You can see the reports for the last 15 and 30 mins also, additional to the already existing time period options
1, 5, 15 Min averages in traffic report	You have an option to view 1,5, 15 mins average data points in the traffic page
Consolidated report for a device	Clicking on the device name / IP address from the interface view will let you drilldown and view the top 10 of interface by speed & utilization, top 10 protocols, applications, source, destination, DSCP, conversation of that particular device.
Localization	NetFlow Analyzer also support Croatian, Spanish, Dutch.

### New Features in Release 7.5

Feature	Description
Customizable dashboard	<b>Users can create dashboard by placing the widgets as per their requirements. This enables easy understanding of the network behavior in one glance</b>
GRE application filter	Applying this filter in any cryptomap tunnel prevents the GRE traffic getting double counted. Otherwise, the cryptomap interface in which NetFlow is enabled double counts the GRE traffic.
Support for MSSQL database	NetFlow Analyzer now supports MSSQL Database also.

Feature	Description
Email option for sending reports	This option allows the user to send a screenshot of a page to a particular mail ID
DSCP names in alerts and IP groups	Now, an user can set alerts based on the DSCP names and also create IP groups to monitor application using particular DSCP names.
Volume based billing	The next level of billing is here, after usage based billing. Users can generate bills based on the volume of data.
Site-to-site traffic monitoring	Users can create groups for monitoring site-to-site traffic.
Secondary DNS server lookup	This allows the system to go through DNS servers other than primary ones for resolving DNS names.
Raw data storage	For users who do not need an in depth report and for whom storing large data is an issue, you can now store the raw data for as less as 1 hour.

## New Features in Release 7.0

Feature	Description
Reporting on Cisco CBQoS	Useful for monitoring class based pre and post policy traffic usage, class based drops and queuing
Authentication using radius server	Useful for centralized controlling of access to resources in a network by a single global set of credentials
Ability to create IP groups with exclude IP address option	One could bulk load IP groups and selectively remove unwanted IP groups
DNS resolving enhancement of source and destination addresses	Faster retrieval of DNS names made possible
Support for user configurable DNS names for IP addresses	Customizable DNS names helps in easier management of the network
Usage based billing	Generation of periodic bills for accounting and for charge-back.
Reporting on source network and destination network	This allows the user to view the source networks, destination networks and conversation between them.
Different IN and OUT speed can be configured for interfaces	Helps in setting appropriate speed for IN and OUT interfaces
Support for exporting reports to CSV	Helps in easier maintenance of data for historical reporting besides the flexibility to import in XLS sheets for any analysis
Sorting on the Autonomous Systems view for easier tracking and for peering arrangement	Ability to group together applications into a single logical entity
Option to exclude ESP_App on user defined interfaces	Ensures that traffic is not double counted in case of ESP tunnels.
Option to suppress output interface accounting on user defined interfaces	Useful when working with WAN accelerators
Quick view traffic graph in Dashboard view	Offers Enhanced usability
Graphs enhanced to one min granularity and also to real-time in Network Snapshot	Offers a more realistic reporting of the network health for quicker action to avoid any network eventuality
Ability to set snmp parameters globally for all routers	Offers the flexibility to avoid havign to set the same SNMP parameters on each individual router
Support for sorting of interfaces based on usage in Dashboard View	Helps in easier viewing of interfaces based on maximum/minimum bandwidth usage and for appropriate action
User management enhanced	Helps individual users to quickly confirm that one's login credentials

Feature	Description
to provide last login time and current login status for all users	have not been compromised
Support for configuring alerts on interface groups.	Interface groups can be used for checking the router traffic (by combining all the interfaces into a single group)
User permission can be granted at a interface group level.	This feature would enable providing permission at an interface level while creating a user.
Look and feel changed	The user interface has been changed for a better user experience
Localization supported	NetFlow Analyzer supports French, German, Chinese and Japanese.

### New Features in Release 6.0

Feature	Description
sFlow Support	Support for sFlow data capture and reporting
Selectable Graph	Option to click and drag on the graph for easier drilldown
Real-Time Reports	Real time reports with graphs. Updates immediately as the data is received
Link Down alert	Alerting feature enhanced to send an alert when link goes down or when no flows are received for 15 minutes
Enhanced Granularity	IN and OUT traffic (in bytes and packets) for each interface maintained with 1 minute granularity for upto 1 year
Performance improvement	Performance improvement in IP group classification engine
Google Map Integration	Integration with Google Maps for a better view of the network
Application Grouping	Ability to group together applications into a single logical entity
DSCP Mapping	Ability to report on DSCP mapping

### New Features in Release 5.5.0

Feature	Description
NBAR based Reporting	NBAR(Network Based Application Recognition) - By intelligent classification of traffic lets you set QoS standard.
Scheduling of Reports	Allows setting of time intervals at which network traffic reports are generated automatically and mailed to desired recipient(s).
NetFlow V9 Support	Basic V9 support.
Associating IP address to application	Associate IP address to an application in addition to port & protocol.
Create Interface Groups	Ability to group interfaces together and monitor traffic.
ToS & TCP_flag	Reports based on TCP flags & TOS can be generated from the Troubleshooting page.

### New Features in Release 5.0

Feature	Description
Threshold-based Alerting	Set up alerts based on link utilization and send emails or SNMP Traps when thresholds are exceeded.
Troubleshooting	Retain raw data for longer time periods (up to 2 weeks) to enable increased visibility into traffic data for troubleshooting and alerts.
Support link	Wide range of options to contact technical support in case of any problems running NetFlow Analyzer.
Enhanced Router Settings	Specify whether router details need to be fetched based on IfName, IfAlias or IfDescription value.
Dashboard View Filter	Filter Dashboard Interface View to display only those interfaces exceeding specific values of incoming or outgoing traffic.

Feature	Description
Traffic Graph Filters	Filter daily and weekly traffic graphs to show hour-based traffic details.
Enhanced IP Group Management	Specify interfaces when creating IP groups to further filter traffic details for an IP group.
Localized Versions	NetFlow Analyzer supports French, German, and Spanish along with Chinese and Japanese.

### Features in Previous Releases (4.0 to 4.0.2)

Feature	Description
Web-based interface	Generate reports and perform administrative tasks from just a web browser
Support for NetFlow export versions	As of release 4.0.2, NetFlow Analyzer includes support for NetFlow version 5 and version 7 exports
Simply "turn on" NetFlow	Simply configure NetFlow export on your router or switch, and see it automatically added on the Dashboard
Real-time Traffic Graphs	View instant graphs of bandwidth utilization per network interface as soon as NetFlow data is received
Historical Trend Reports	Generate daily, weekly, monthly, and custom time period bandwidth reports showing peak traffic patterns
Bandwidth Usage Reports	View reports showing top applications, top hosts, and top conversations using bandwidth
Consolidated Reports	View bandwidth reports per interface, showing all details on bandwidth usage for that interface
Autonomous Systems Reports	View AS and peering information for routers configured with BGP (useful for service providers)
NetFlow Devices	Categorize devices exporting NetFlow into logical groups and monitor them exclusively
IP Groups	Create departments based on IP addresses, ports, protocols, or interfaces and generate specific bandwidth usage reports
Application Configuration	Identify most standard applications out-of-the-box and configure custom applications to recognize specific traffic
User management	Add users with different privileges, assign device groups, and selectively allow access
Localized setup	NetFlow Analyzer can be installed and run in Chinese and Japanese languages, with support for more languages being added frequently. Check the website for the latest list of languages localized, and also contribute to translation works.

# Installation and SetUp

## System Requirements

This section lists the minimum requirements for installing and working with NetFlow Analyzer.

### Hardware Requirements

The minimum hardware requirements for NetFlow Analyzer to start running are listed below.

- 2.4GHz, Pentium 4 processor, or equivalent
- 1GB RAM
- 10GB disk space for the database

Interface	Processor	RAM	Hard-disk space
Upto 10 (low end routers)	2.6 GHz P-D/ 3.0 GHz P4 HT or equivalent	1 GB	20 GB
11 - 25	2.8 GHz P-D or equivalent	1 GB	40 GB
26 - 50	2.6 GHz Core 2 Duo or equivalent	1 GB	60 GB
51 - 100	3.0 GHz Core 2 Duo / 2.4 GHz dual core Xeon 3000 series or equivalent	2 GB	75 GB
101 - 300	2.6 GHz <b>dual core</b> 3000 series Xeon Processor or equivalent	4 GB	225 GB
301 - 600	2.6 GHz <b>quad core</b> 3000 series Xeon Processor or equivalent	4 GB	450 GB

NetFlow Analyzer is optimized for 1024 x 768 resolution and above.



For the device exporting NetFlow, ensure that the NetFlow export version format is exactly the same as the Cisco NetFlow version 5 or version 7 or version 9 format. For information on Cisco devices and IOS versions supporting Netflow, consult the Cisco NetFlow Device Support table.

### Software Requirements

#### Platform Requirements

NetFlow Analyzer can be installed and run on the following operating systems and versions:

- Windows 2000 Server/Professional with SP 4
- Windows XP with SP 1
- RedHat Linux 8.0, 9.0
- SUSE Linux

## **Supported Web Browsers**

NetFlow Analyzer has been tested to support the following web browsers and versions:

- Internet Explorer 5.5 and later
- Netscape 7.0 and later
- Mozilla 1.5 and later

## Prerequisites

---

Before setting up NetFlow Analyzer in your enterprise, ensure that the following are taken care of.

### Ports Required

NetFlow Analyzer requires the following ports to be free:

Port Name	Default Port Number	Usage
Web server port	8080	This is the port on which you will connect to the NetFlow Analyzer server from a web browser. You can change this at any time from the Settings tab.
NetFlow Listener port	9996	This is the port on which NetFlow exports are received from routers. You can change this at any time from the Settings tab.
MySQL port	13310	This is the port used to connect to the MySQL database in NetFlow Analyzer. Changing this port requires configuration level changes.

### Recommended System Setup

Apart from the System Requirements, the following setup would ensure optimal performance from NetFlow Analyzer.

- Run NetFlow Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor can cause problems in collecting NetFlow data.
- Use the MySQL pre-bundled with NetFlow Analyzer that runs on port 13310. You need not start another separate instance of MySQL.

### Changing the Default MySQL Port

1. Edit the `mysql-ds.xml` file present in the `<NetFlowAnalyzer_Home>/server/default/deploy` directory.
2. Change the port number in the following line to the desired port number:  
`<connection-url>jdbc:mysql://localhost:13310/netflow</connection-url>`
3. Save the file and restart the server.

## Installing and Uninstalling

---

NetFlow Analyzer is available for Windows and Linux platforms. For information on supported versions and other specifications, look up System Requirements.

### Installing NetFlow Analyzer

#### Windows:

The Windows download for NetFlow Analyzer is available as an EXE file at <http://www.netflowanalyzer.com/download.html>  
Download the EXE file to your local machine, and double-click it to start installation. Follow the instructions as they appear on screen to successfully install NetFlow Analyzer on to your machine.

#### Linux:

The Linux download for NetFlow Analyzer is available as a BIN file at <http://www.netflowanalyzer.com/download.html>

1. Download the BIN file and assign **execute** permission using the command: `chmod a+x <file_name>.bin`  
where `<file_name>` is the name of the downloaded BIN file.
2. Execute the following command: `./<file_name>.bin`



During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the `-is:tempdir <directoryname>` option, where `<directoryname>` is the absolute path of an existing directory.  
`./<file_name>.bin -is:tempdir <directory_name>`

Follow the instructions as they appear on the screen to successfully install NetFlow Analyzer on to your machine.

### Uninstalling NetFlow Analyzer

#### Windows

1. Navigate to the Program folder in which NetFlow Analyzer has been installed. By default, this is **Start > Programs > ManageEngine NetFlow Analyzer**
2. Select the option **Uninstall NetFlow Analyzer**
3. You will be asked to confirm your choice, after which NetFlow Analyzer is uninstalled

#### Linux

1. Navigate to the `<NetFlowAnalyzerHome>/_uninst` directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which NetFlow Analyzer is uninstalled.

## Starting and Shutting Down

---

Once you have successfully installed NetFlow Analyzer, start the NetFlow Analyzer server by following the steps below.

### Starting NetFlow Analyzer

#### Windows:

Click on **Start > Programs > ManageEngine NetFlow Analyzer > NetFlow Analyzer** to start the server.

Alternatively you can navigate to the `<NetFlowAnalyzer_Home>\bin` folder and invoke the **run.bat** file.

#### Linux:

Navigate to the `<NetFlow Home>/bin` directory and execute the **run.sh** file.

When the server is started, a command prompt window opens up showing startup information on several modules of NetFlow Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.
Please connect your client at http://localhost:8080
```

where 8080 is replaced by the port you have specified as the web server port during installation.

### Starting as Service

#### Windows:

If you have chosen the **Start as Service** option during installation, NetFlow Analyzer will run as a service on Windows.

#### Linux:

1. Login as root user.
2. Navigate to the `<NetFlowAnalyzer_Home>\bin` directory.
3. Execute the **linkAsService.sh** file
4. Then execute the command `/etc/init.d/netflowanalyzer start`

This starts NetFlow Analyzer as a service on Linux.

As far as **Fedora / SUSE** is concerned, please open the **mysql-ds.xml** file under the `server\default\deploy` directory and change the

```
</connection-url> to
```

```
</connection-url>
```

and restart the NetFlow Analyzer server.

Please follow the instructions below,

1. Navigate to /bin folder and backup (copy) linkAsService.sh to a safe location.
2. Open file linkAsService.sh in a editor and look for the following lines,

```
[code:1:f5099fc2e0]for i in {0,6}
do
ln -s -f $initvar /etc/rc$i.d/$stopwith
done
ln -s -f $initvar /etc/rc5.d/$startwith[/code:1:f5099fc2e0]
```

3. Edit the above lines as follows, suffixing rc.d folder after /etc/ folder,

```
[code:1:f5099fc2e0]for i in {0,6}
do
ln -s -f $initvar /etc/rc.d/rc$i.d/$stopwith
done
ln -s -f $initvar /etc/rc.d/rc5.d/$startwith
[/code:1:f5099fc2e0]
```

4. Save the file.
5. Shutdown NetFlow Analyzer.

Execute linkAsService.sh and start NetFlow Analyzer using the command \"  
/etc/init.d/netflowanalyzer start \"

## Shutting Down NetFlow Analyzer

Follow the steps below to shut down the NetFlow Analyzer server. Please note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by NetFlow Analyzer are freed.

### Windows:

1. Navigate to the Program folder in which NetFlow Analyzer has been installed. By default, this is **Start > Programs > ManageEngine NetFlow Analyzer**
2. Select the option **Shut Down NetFlow Analyzer**
3. Alternatively, you can navigate to the <NetFlowAnalyzer\_Home>\bin folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the NetFlow Analyzer server is shut down.

### Linux:

1. Navigate to the <NetFlowAnalyzer\_Home>/bin directory.
2. Execute the shutdown.sh file.
3. You will be asked to confirm your choice, after which the NetFlow Analyzer server is shut down.

## Accessing the Web Client

---

NetFlow Analyzer is essentially a bandwidth monitoring tool that uses Cisco NetFlow exports to analyze network traffic and determine bandwidth usage.

Once the server has successfully started, follow the steps below to access NetFlow Analyzer.

1. Open a supported web browser window
2. Type the URL address as **http://<hostname>:8090** (where **<hostname>** is the name of the machine on which NetFlow Analyzer is running, and **8090** is the default web server port)
3. Log in to NetFlow Analyzer using the default username/password combination of **admin/admin**

Once you log in, you can start managing devices exporting Cisco NetFlow, generate bandwidth reports, and more.

## License Information

---

NetFlow Analyzer comes in two flavors:

- **Free Edition** - collect, analyze, and report on Netflow data from a maximum of **two** interfaces
- **Professional Edition** - collect, analyze, and report on Netflow data from a maximum of n interfaces (where 'n' is the number of interfaces for which NetFlow Analyzer has been purchased)
- **Professional Plus Edition** - It has all the features of professional edition + reporting on Cisco CBQoS, Cisco NBAR and usage based billing

Once installed, NetFlow Analyzer runs in evaluation mode for 30 days. You can obtain a registered license for NetFlow Analyzer at any time during the evaluation period by contacting NetFlow Analyzer Support.

If you have not upgraded to the Professional Edition by the end of the evaluation period, NetFlow Analyzer automatically reverts to the Free Edition.

### Upgrading your License

After obtaining the new license from ZOHO Corp, save it on your computer, and follow the steps below to upgrade your NetFlow Analyzer installation:

1. Log in to the NetFlow Analyzer web client
2. Click **License Management** from Admin Operations
3. Click the **Upgrade License** link present in the top-right corner of the screen
4. In the License window that opens up, browse for the new license file and select it
5. Click **Upgrade** to apply the new license file



The new license is applied with immediate effect. You do not have to shut down or restart the NetFlow Analyzer server after the license is applied.

## Configuring Flow Exports

### Devices and Supported Flow exports

---

The following chart specifies information on the various vendors and the flow exports their devices support. Click on the specific device name to know how to configure the corresponding flow export.

Device/Vendor	Supported Flow Export
Cisco	NetFlow
Juniper Devices	cflowd, jFlow
Nortel	IPFIX
Huawei, 3com, H3C	Netstream
Alcatel-Lucent, Extreme Networks, Foundry Networks, HP, Hitachi, NEC, AlaxalA Networks, Allied Telesis, Comtec Systems, Force10 Networks	sFlow

## Cisco Devices (NetFlow)

### Configuring Cisco Devices

---

This section offers a brief guide to setting up NetFlow on a Cisco router or switch. For more detailed information, refer the Cisco web site at <http://www.cisco.com/go/netflow>. It is recommended that only people with experience in configuring Cisco devices follow these steps.

- Cisco devices with NetFlow support
- Configuring an IOS Device
- Configuring a Catalyst 6000 Series Switch
- Configuring a Native IOS Device
- Configuring a Catalyst 4000 Series Switch

Configuring NetFlow for BGP

#### Setting the appropriate time on the router

NetFlow Analyzer stamps the flows based on the router time. It is therefore important to ensure that the time on the router is set properly. Netflow Analyzer can handle routers from different time zones automatically, provided the correct time is set.

Whenever the time difference between the NetFlow Analyzer Server and the router is above 10 minutes a warning icon will appear in the home page. When this happens, NetFlow Analyzer will stamp the flows based on the system time of the NetFlow Analyzer server.

In case you see this, please ensure the following on the router:

- Check if the correct time is set on your router. You can check this by logging into the router and typing **show clock**. You can set the clock time using the command **clock set hh:mm:ss date month year**. [ An example : **clock set 17:00:00 27 March 2007** ]
- Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the configure terminal and typing **show running-config**. You can set the clock time zone and offset using the command **clock timezone zone hours [minutes]** (E.g. clock timezone PST -8 00)



To enable NetFlow in an MPLS environment refer Cisco's documentation on MPLS NetFlow

## Cisco® NetFlow Device Support

The following charts include information on the various vendors and devices supporting NetFlow version 5 or 7 or 9 data export. Use these charts to determine if your devices are compatible with NetFlow Analyzer.

### Cisco Routers

Cisco IOS Software Release Version	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	Cisco 7200 and 7500 series, RSP 7200 series
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series
12.0T, 12.0S	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8600 series
12.0(3)T, 12.0(3)S	Cisco 1720, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)T	Cisco 1400, 1600, 1720, 2500, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)XE	Cisco 7100 series
12.0(6)S	Cisco 12000 series

NetFlow is also supported by these devices Cisco 800, 1700, 1800, 2800, 3800, 6500, 7300, 7600, 10000, CRS-1 and these Catalyst series switches: 45xx, 55xx, 6xxx.



**These devices do not support NetFlow: Cisco 2900, 3500, 3660, 3750.**

### Cisco Switches

NetFlow export is also supported on other Cisco switches when using a NetFlow Feature Card (NFFC) or NFFC II and the Route Switch Module (RSM), or Route Switch Feature Card (RSFC). However, check whether version 5 is supported, as most switches export version 7 by default.

### NetFlow Version 9 Support

#### Supported Platforms

The following platforms support NetFlow Version 9 Data Export :

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7300 series

- Cisco 7400 series
- Cisco 7500 series
- Cisco 12000 series

## **Other Vendors**

Some of the major vendors supporting NetFlow include:

- **3Com** - 8800 Series Switches
- **Adtran** - NetVanta 3200, 3305, 4305, 5305, 1524, 1624, 3430, 3448, 3130, 340, and 344. (Supports NetFlow version 9)
- **Juniper Networks** - Does not support sampling interval attribute. First and last times are stored in seconds rather than milliseconds
- **Riverbed**
- **Enterasys Networks**
- **Extreme Networks** - Does not support input/output interface, octets, or first and last times
- **Foundry Networks**

## Configuring Cisco ASA 5500 series

---

ASA NetFlow export is dependent on the version of ASA software running. ASA version 8.2 software supports NetFlow export across all ASA models. The following fields must be included in the ASA configuration to export flow data to the NetFlow Analyzer .

The following commands must be included in your global service policy for NetFlow export to function.

```
(config)# flow-export destination inside NetFlow Analyzer server IP address 9996
(config)# flow-export template timeout-rate 1
(config)# flow-export delay flow-create 60
(config)# logging flow-export syslogs disable
(config)# access-list netflow-export extended permit ip any any
(config)# class-map netflow-export-class
(config-cmap)#match access-list netflow-export
(config)# policy-map netflow-export-policy
(config-pmap)# class netflow-export-class
(config-pmap-c)# flow-export event-type any destination NetFlow Analyzer server IP

(config)#service-policy netflow_export_policy global
```

For more clarification regarding this, please go to  
<http://forums.manageengine.com/#topic/49000003577055>

## Configuring NetFlow Export on an IOS Device

Follow the steps below to configure NetFlow export on a Cisco IOS device.



Refer the Cisco Version Matrix for information on Cisco platforms and IOS versions supporting NetFlow

### Enabling NetFlow Export

Enter global configuration mode on the router or MSFC, and issue the following commands for **each interface** on which you want to enable NetFlow:

```
interface {interface} {interface_number}
ip route-cache flow
bandwidth <kbps>
exit
```



In some recent IOS releases Cisco Express Forwarding has to be enabled. Issue the command **ip cef** in global configuration mode on the router or MSFC for this.

This enables NetFlow on the specified interface alone. Remember that on a Cisco IOS device, **NetFlow is enabled on a per-interface basis**. The `bandwidth` command is optional, and is used to set the speed of the interface in kilobits per second. Interface speed or link speed value is used to later calculate percentage utilization values in traffic graphs.

### Exporting NetFlow Data

Issue the following commands to export NetFlow data to the server on which NetFlow Analyzer is running:

Command	Purpose
<code>ip flow-export destination {hostname ip_address} 9996</code>	Exports the NetFlow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured NetFlow listener port. The default port is 9996.
<code>ip flow-export source {interface} {interface_number}</code>	Sets the source IP address of the NetFlow exports sent by the device to the specified IP address. NetFlow Analyzer will make SNMP requests of the device on this address.
<code>ip flow-export version 5 [peer-as   origin-as]</code>	Sets the NetFlow export version to version 5. <b>NetFlow Analyzer supports only version 5, version 7 and version 9</b> . If your router uses BGP you can specify that either the origin or peer AS is included in exports - it is not possible to include both.
<code>ip flow-cache timeout active 1</code>	Breaks up long-lived flows into 1-minute fragments. You can choose any number of minutes between 1 and 60. If you leave it at the default of 30 minutes your traffic reports will have spikes. It is important to set this value to <b>1 minute</b> in order to generate alerts and view troubleshooting data.
<code>ip flow-cache timeout inactive 15</code>	Ensures that flows that have finished are periodically exported. The default value is 15 seconds. You can choose any number of seconds between 10 and 600. However, if you choose a value greater than 250 seconds, NetFlow Analyzer may report traffic levels that are too low.
<code>snmp-server ifindex persist</code>	Enables ifIndex persistence (interface names) globally. This ensures that the ifIndex values are persisted during device reboots.



For more information on BGP reporting in NetFlow Analyzer, look up the section on Configuring NetFlow for BGP

## Verifying Device Configuration

Issue the following commands in **normal (not configuration) mode** to verify whether NetFlow export has been configured correctly:

Command	Purpose
show ip flow export	Shows the current NetFlow configuration
show ip cache flow	These commands summarize the active flows and give an indication of how much NetFlow data the device is exporting
show ip cache verbose flow	


## A Sample Device Configuration

The following is a set of commands issued on a router to enable NetFlow version 5 on the FastEthernet 0/1 interface and export to the machine 192.168.9.101 on port 9996.

```

router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination 192.168.9.101 9996
router-2621(config)#ip flow-export source FastEthernet 0/1
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
    
```

*\*repeat these commands to enable NetFlow for each interface*




**Please note that NetFlow data export has to be enabled on all interfaces of a router in order to see accurate IN and OUT traffic.** Suppose you have a router with interface A and B. Since NetFlow, by default, is done on an ingress basis, when you enable NetFlow data export on interface A, it will only export the IN traffic for interface A and OUT traffic for interface B. The OUT traffic for interface A will be contributed by the NetFlow data exported from interface B.

Even if you are interested in managing only interface A, please enable NetFlow data export on A and B. You may subsequently unmanage interface B from the License Management link.

## Turning off NetFlow

Issue the following commands in global configuration mode to stop exporting NetFlow data:

Command	Purpose
no ip flow-export destination {hostname ip_address} {port_number}	This will stop exporting NetFlow cache entries to the specified destination IP address on the specified port number
interface {interface} {interface_number}	This will disable NetFlow export on the specified interface. Repeat the commands for each interface on which you need to disable NetFlow.
no ip route-cache flow	
exit	



For further information on configuring your IOS device for NetFlow data export, refer Cisco's NetFlow commands documentation

## Configuring NDE on Catalyst 6000 Series Switches

Follow the steps below to configure NDE on Catalyst 6000 Series switches

### Configuring NDE on Catalyst 6000 Series Switches

Enter privileged mode on the Supervisor Engine and issue the following commands to configure NDE:

Command	Purpose
set mls nde {hostname ip_address} 9996	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of hardware-switched packets.
ip flow-export destination {hostname ip_address} 9996	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of software-switched packets. *
set mls agingtime long 64	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to <b>1 minute</b> in order to generate alerts and view troubleshooting data.
set mls agingtime 32	Ensures that flows that have finished are periodically exported. Ensure that the set value is not too low, else NetFlow Analyzer may report traffic levels that are too low.
set mls flow full	This sets the flow mask to full flows. This is required to get useful information from the switch.
set mls nde enable	This enables NDE

*\*To monitor data and statistics about Layer 3 traffic that is switched in software by the MSFC, you must specify the NDE collector and UDP port on the MSFC. This requires that you enter the `ip flow-export destination` command on the MSFC.*



Use the `show mls debug` command to debug the NDE configuration



For more information on configuring NDE on Catalyst 6000 Series switches, refer Cisco's documentation.

## Configuring NDE on a Native IOS Device

To enable NDE on a Native IOS device, enter the configure mode on the Supervisor Engine, and follow the instructions for an IOS device. Then issue the following commands to enable NDE.


### Configuring NDE

Enter privileged mode on the Supervisor Engine and issue the following commands to enable NDE:

Command	Purpose
mls nde sender version 7	Sets the export version. Version 7 is the most recent full export version supported by switches.
set mls aging long 64	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to <b>1 minute</b> in order to generate alerts and view troubleshooting data.
set mls aging normal 32	Ensures that flows that have finished are periodically exported. A lower value may result in NetFlow Analyzer reporting traffic levels that are too low.

In order to put interface an routing information into the Netflow exports, issue the following commands depending on the Supervisor Engine.

Switch Configuration	Lowest IOS (MSFC) Level	Commands
Sup2 or 720	12.1.13(E)	mls flow ip interface-full mls nde interface
Sup1	12.1.13(E)	set mls flow ip full

	This information is not available with IOS versions earlier than 12.1.13(E) on the Supervisor Engine 2 or 720
---	---

## Configuring NDE on 4000 Series Switches

---

Follow the steps below to configure NDE on a 4000 Series switches.



The 4000 and 4500 series switches require a Supervisor IV or a Supervisor Engine V with a NetFlow Services daughter card (WS-F4531) and IOS version 12.1(19)EW or above to support NDE. Or you must have the Supervisor Engine V-10GE (the functionality is embedded in the supervisor engine).

Configure this device as for an IOS device, but **omit** the `ip route-cache flow` command on each interface. Then issue the following command:

```
ip route-cache flow infer-fields
```

This command ensures routing information is included in the flows. You will not enter the `ip route-cache flow` command on each interface.

### A Sample Device Configuration

The following is a set of commands issued on a 4000 Series switch to enable NetFlow version 7 and export to the machine 192.168.9.101 on port 9996 using FastEthernet 0/1 as the source interface.

```
switch>(enable)ip flow-export destination 192.168.9.101 9996
switch>(enable)ip flow-export version 7
switch>(enable)ip flow-export source FastEthernet 0/1
switch>(enable)ip flow-cache timeout active 1
switch>(enable)ip route-cache flow infer-fields
```

## Configuring NetFlow for BGP

The Border Gateway Protocol (BGP), defined in RFC 1771, provides loop-free interdomain routing between autonomous systems. (An autonomous system [AS] is a set of routers that operate under the same administration.) BGP is often run among the networks of Internet service providers (ISPs).



In order to get AS info, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.

### Enabling BGP Routing

Enter the global configuration mode and issue the following commands to enable BGP routing and establish a BGP routing process:

Command	Purpose
<code>router bgp as-number</code>	Enables the BGP routing process, which places the router in router configuration mode
<code>network network-number [mask network-mask] [route-map route-map-name]</code>	Flags a network as local to this autonomous system and enters it to the BGP table

### Configuring BGP Neighbors

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, issue the following command in router configuration mode:

Command	Purpose
<code>neighbor {ip-address peer-group-name} remote-as as-number</code>	Specifies a BGP neighbor

### BGP Neighbor Configuration Examples

The following example shows how BGP neighbors on an autonomous system are configured to share information.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighboring routers. The first router listed is in a different autonomous system; the second neighbor's `remote-as` router configuration command specifies an internal neighbor (with the same autonomous system number) at address 131.108.234.2 and the third neighbor's `remote-as` router configuration command specifies a neighbor on a different autonomous system.

## Including AS Info in Netflow Exports

If you have configured BGP on your network, and want Netflow to report on autonomous systems (AS info), issue the following command on the router in global configuration mode:

Command	Purpose
<code>ip flow-export destination {hostname ip_address} 9996</code>	Exports the Netflow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured Netflow listener port. The default port is 9996.
<code>ip flow-export {version}[peer-as   origin-as]</code>	Exports NetFlow cache entries in the specified version format (5 or 7). If your router uses BGP, you can specify that either the origin or peer ASs are included in exports – it is not possible to include both.

## Juniper Devices (cflowd/J-Flow)

### Configuring flow exports on Juniper Routers

This section gives the steps to configure cflowd/J-Flow export on Juniper devices. To enable sampling and to export the flow records to specific destination address, follow the below command:

```
forwarding-options {
  sampling {
    input {
      family inet {
        rate 100;
        run-length 9;
        max-packets-per-second 7000;
      }
    }
    output {
      cflowd <destination address>{
        port <port number>;
        source-address <source address>;
        version <version number>;
        no-local-dump;
        autonomous-system-type origin;
      }
    }
  }
}
```

To enable packet sampling on the particular interface(s), from which flow analysis to be done follow the below steps:

```
interfaces {
  ge-1/3/0 {
    vlan-tagging;
    unit 101 {
      vlan-id 101;
      family inet {
        sampling {
          input;
          output;
        }
      }
      address 206.80.253.26/25
    }
  }
}
```

For more information, refer here and this link ([to configure V9 Template record](#)).

## Huawei/3com devices(Netstream)

### Configuring NetStream Export

---

#### On H3C routers:

Please refer to this link to configure Netstream exports on H3C devices.

#### On Huawei Devices:

Follow the below command to enable NetStream on Huawei devices

```
ip netstream export host {hostname|ip_address}
9996
```

This exports the NetStream exports to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured listener port. The default port is 9996.

```
ip netstream export source interface {interface
name}
```

Sets the source IP address of the NetStream exports sent by the device to the specified IP address. NetFlow Analyzer will make SNMP requests of the device on this address. For enabling Netstream on the desired interface, please execute the following command

```
ip netstream inbound
```

## Nortel Devices(IPFIX)

### Configuring IPFIX Export

---

According to Nortel Devices, Internet Protocol Flow Information eXport (IPFIX) has evolved as an improvement upon the Netflow V9 protocol. *It is an upcoming standard that has been proposed by an IETF Working Group - <http://www.ietf.org/html.charters/ipfix-charter.html>. IPFIX is an effort to standardize on architecture for IP flow measurement and export. In an IPFIX model, an exporter such as a switch or router collects IP flows and then exports the IP flow information using a transport protocol to a collection server or servers. An IP flow is defined as a set of packets over a period of time that has some common properties.*

Please refer to the PDF document published by Nortel Devices in this page to configure IPFIX flow exports from your Nortel Devices.

## sFlow exporting devices

### sFlow Reporting

---

#### What is sFlow ?

According to sFlow.org, *sFlow® is an industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats.*

It further says, *sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution:*

- **sFlow is an industry standard** with interoperable implementations provided by a wide range of network equipment and software application vendors
- **sFlow provides a network-wide view** of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location
- **sFlow is scalable**, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load
- **sFlow is a low cost solution.** It has been implemented on a wide range of devices, from simple L2 workgroup switches to high-end core routers, without requiring additional memory and CPU

## sFlow Supported Devices

### Which devices support sFlow ?

The following devices are capable of exporting sFlow :

#### AlaxalA Networks

- AX7800R
- AX7800S
- AX7700R
- AX5400S

#### Alcatel

- OmniSwitch 6850
- OmniSwitch 9000

#### Allied Telesis

- SwitchBlade 7800R series
- SwitchBlade 7800S series
- SwitchBlade 5400S series

#### Comtec Systems

- !-Rex 16Gi & 24Gi & 24Gi-Combo

#### Extreme Networks

- Alpine 3800 series
- BlackDiamond 6800 series
- BlackDiamond 8800 series
- BlackDiamond 10808
- BlackDiamond 12804C
- BlackDiamond 12804R
- Summit X450 Series
- Summit i series

#### Force10 Networks

- E series

#### Foundry Networks

- BigIron series
- FastIron series
- IronPoint series
- NetIron series
- SecureIron series
- ServerIron series

#### Hewlett-Packard

- ProCurve 2800 series
- ProCurve 3400cl series
- ProCurve 3500yl series

- ProCurve 4200vl series
- ProCurve 5300xl series
- ProCurve 5400zl series
- ProCurve 6200yl series
- ProCurve 6400cl series
- ProCurve 9300m series
- ProCurve Routing Switch 9408sl

**Hitachi**

- GR4000
- GS4000
- GS3000

**NEC**

- IP8800/R400 series
- IP8800/S400 series
- IP8800/S300 series

## Enabling sFlow

### How do I enable sFlow ?

If your device supports sFlow, then you will have to enable sFlow on each of the interfaces that you want to collect flow statistics on.

### Enabling sFlow on various devices

#### Foundry Networks switch

```
foundry2402#enable
Password:*****
foundry2402#configure terminal
foundry2402(config)# interface ethernet 10
foundry2402(config-if-e100-10)#sflow forwarding
foundry2402(config-if)#exit foundry2402(config)# sflow enable
foundry2402(config)# sflow destination 192.168.0.2 9996
foundry2402(config)# sflow sample 256
foundry2402(config)# sflow polling-interval 10
```



Please note that the part in red has to be repeated for each interface individually. For more information on Foundry devices configuration refer to [www.foundrynet.com](http://www.foundrynet.com)

#### Force10 switch

```
force#enable
Password:*****
force#configure terminal
force(config-interface)#sflow enable
[ This command has to be repeated for all interfaces. ]
force(config)#sflow destination 192.168.0.2 9996 agent-addr 192.168.1.2
force(config)# sflow sample 256
force(config)# sflow polling 10
```

For more information on Force10 devices refer to [www.force10networks.com](http://www.force10networks.com)

#### Extreme Networks switch

Please refer to the following documentation for configuring sFlow on Extreme Networks switch

- [http://www.extremenetworks.com/libraries/whitepapers/WPsFlow\\_1247.pdf](http://www.extremenetworks.com/libraries/whitepapers/WPsFlow_1247.pdf)
- For enabling sFlow on the port use the following command. This has to be repeated for all the ports.

```
extreme#enable sflow port 2
```

For more information on Extreme Network devices refer to [www.extremenetworks.com](http://www.extremenetworks.com)

#### Hewlett-Packard ProCurve switches

```
hp#enable
Password:*****
hp#configure terminal
hp# sflow 1 sampling A1,A2,A2 256 [ sflow 1 sampling <modules> <sampling rate>]
hp# sflow 1 destination 192.168.0.2 9996
```

The above commands work only on latest HP devices.

sFlow can be enabled on some of the HP switches only through SNMP. We provide two script files for enabling and disabling sFlow on HP switch.

The script files **SFlowEnable.bat** / **SFlowEnable.sh** and **SFlowDisable.bat** / **SFlowDisable.sh** are present under <NFA\_HOME>/troubleshooting folder.

For **enabling sFlow** you need to provide the below command:

```
SFlowEnable.bat switchIp snmpPort snmpWriteCommunity collectorIP collectorPort  
samplingRate
```

An example,

```
SFlowEnable.bat Hp2824 161 private 192.168.3.1 9996 256
```

For **disabling sFlow** you need to provide the below command:

```
SFlowDisable.bat switchIp snmpPort snmpWriteCommunity
```

An example,

```
SFlowDisable HpProcurve 161 private
```

For more information on HP devices refer to [www.hp.com](http://www.hp.com)

## Getting Started

---

Once NetFlow Analyzer has been successfully set up and started in your network, the next thing to do is to start receiving Netflow exports from routing devices on your network.




The Configuring Cisco Devices section contains useful information on how to configure Netflow export on different Cisco routers and switches. The sFlow section contains useful information on configuring sFlow.

As soon as you log in to the NetFlow Analyzer web client, you will see the **Global View - Dashboard View**. This view shows you information on interfaces sending Netflow and sFlow exports, AS info, as well as traffic information for all IP groups created so far. The Dashboard is populated as soon as Netflow or sFlow data is received from any interface.

The Global View is divided into three tabs

1. The **Network Snapshot View** which lists the top devices, top interfaces and top IP Groups
2. The **Interface View** which lists all the interfaces from which Netflow or sFlow exports are received
3. The **Autonomous System View** which lists all the autonomous systems configured with each router

From any tab, click the  icon to return to the Global View.

## Dashboard view

By default you can view the **Network snapshot**. You can also customize the dashboard as per your own requirements.

### Customizable dashboard:


The dashboard can be customized by users to display widgets of their own choice. To create a new dashboard view, click on "Actions" on the top right. In the dropdown click on "new dashboard".


Fill in the Information:


Title	Description
Name	The name of the dashboard view
Description	Describe this view for easy reference and understanding
No. of columns	No. of columns the user wants to be displayed in this dashboard view. It can be 1,2 or 3. And the the numbers below with "%" gives the width of the page allocated to the particular column.
Widgets	Select the widgets that needs to be displayed in the dashboard

Click "**Save**" to save this particular dashboard view. It can be later **edited**, at any time, by going to the particular dashboard view and clicking on "Actions" on the top right. In the dropdown click on either "**Edit layout**" if the need is to change the name, layout, description **OR** click on "**Add Widgets**" to add additional widgets.

Once the view is saved, the particular dashboard will be displayed. You can move the widgets as per your wish by dragging and dropping the widget at another place.

You can "**reload**" a particular widget by clicking on "".

You can **delete** a dashboard view by clicking on "Actions" on the top right. In the dropdown click on "**Delete**". This deletes the current dashboard view. Yo can also delete a particular widget in the dashboard by clicking on "" of the particular widget.

You can **configure / edit** a widget by clicking on configure or "". You can edit the following

Title	Description
Name	The name of the widget
Period	You can select the period (from the dropdown box) for which you need to monitor.
Show only	Select the top "N" to be seen
Refresh time	Set the refresh time from the dropdown box.

And "**Save**" the changes.

Your dashboard view is all ready!

While drilling down an interface, you can directly jump to the any dashboard view by clicking on the "**Dashboard**" on the top right. In the dropdown, select the name of the dashboard you wish to view.

You can toggle between various views by clicking on the "Dashboards" on the top right. In the dropdown click the dashboard that you want to view.

### Network snapshot

The **Network Snapshot View** is the default view when the user logs in to NetFlow Analyzer application. The time period for which the report is shown can be modified using the **Select Period** .

The time period chosen could be one of - Last Hour, Last 6 Hours, Today and Last 24 Hours.

It displays details categorized under the following heads.

1. Top Devices by Speed
2. Top Interfaces by Speed
3. Top Interfaces by Utilization
4. Top IP Groups by Speed
5. Top IP Groups by Utilization

The top 5 Interfaces/ IP groups are listed in each category, as the case may be.

**Top Devices by Speed**

The Top Devices by Speed categorization lists the top 5 devices ( routers/switches ) on the basis of speed. is shown against each device name. Details of the Maximum Speed, Average Speed, Average Voulme, percentage utilization is shown against each device name. The Pie chart gives the representation of the share of the top devices as a percentage. Clicking on the region of a pie-chart gives details at the interface level for the device chosen. The same can be seen by clicking on the Device Name listed under the heading **Device Name**. The rectangular plot alongside the piechart gives the 1 Minute Average plot of speed Vs time.

**Top Interfaces by Speed**

The Top Interfaces by Speed categorization lists the top 5 interfaces ( globally ) on the basis of speed. Details such as the Device Name( on which the interface resides), the In and Out speeds on the Interface are listed. By clicking on any Interface Name, it is possible to further drill down to see more details on speed related information on this interface.

**Top Interfaces by Utilization**

The Top Interfaces by Utilization categorization lists the top 5 interfaces ( globally ) on the basis of Utilization. Details such as the Device Name( on which the interface resides), the In and Out Utilization on the Interface are listed. By clicking on any Interface Name, it is possible to further drill down to see more details on the utilization information on this interface.


**Top IP Groups by Speed**

The Top IP Groups by Speed categorization lists the top 5 IP Groups ( globally ) on the basis of speed. Details on the In and Out speeds on the IP Group are listed. By clicking on any IP Group Name, it is possible to further drill down to see more speed related details on the IP Group.

**Top IP Groups by Utilization**

The Top IP Groups by Utilization categorization lists the top 5 IP Groups ( globally ) on the basis of Utilization. Details on the In and Out utilization values on the IP Groups are listed. By clicking on any IP Group Name, it is possible to further drill down to see more utilization related details on the IP Group

The purpose of icons and buttons in the Network Snapshot View is explained below.

Icon/ Button	Purpose
 (near Refresh this page)	Click this icon, to set the time period for refreshing the page contents.

## Dashboard view

---

Dashboard can also be created by "operator" and " guest" privilege users.

### Configuring the dashboard:

The dashboard can be customized by users to display widgets of their own choice. To create a new dashboard view, click on "Actions" on the top right. In the dropdown click on "new dashboard".

Fill in the Information:

Title	Description
Name	The name of the dashboard view
Description	Describe this view for easy reference and understanding
No. of columns	No. of columns the user wants to be displayed in this dashboard view. It can be 1,2 or 3. And the the numbers below with "%" gives the width of the page allocated to the particular column.
Widgets	Select the widgets that needs to be displayed in the dashboard

### Widgets:

Select the required widgets from the list on the right. It consists the four critical parameters one needs to monitor:

1. **Device** - This lets the user monitor the top N devices / interfaces by speed, volume and other listed parameters. The "N" can be either 5 or 10 and can be configured in the dashboard view, after creating the dashboard.
2. **Interface** - This lets the user monitor the top N source / destination / conversation / application and many more by IN / OUT, for a particular interface, which can be configured in the dashboard view, after creating the dashboard.
3. **Interface group** - This lets the user monitor the top N source / destination / conversation / application and many more by IN / OUT, for a particular interface group, which can be configured in the dashboard view, after creating the dashboard.
4. **IP group** - This lets the user monitor the top N source / destination / conversation / application and many more by IN / OUT, for a particular IP group, which can be configured in the dashboard view, after creating the dashboard.



The "N" can be either 5 or 10 and can be configured through the dashboard view, after creating the dashboard.

Click "**Save**" to save this particular dashboard view. It can be later **edited**, at any time, by going to the particular dashboard view and clicking on "Actions" on the top right. In the dropdown click on either "**Edit layout**" if the need is to change the name, layout, description **OR** click on "**Add Widgets**" to add additional widgets.


Once the view is saved, the particular dashboard will be displayed. You can move the widgets as per your wish by dragging and dropping the widget at another place.

## Dashboard Interface View

The **Interface View** tab displays information on all interfaces from which NetFlow exports are received.









The default **Router List** shows all the routers and interfaces from which NetFlow exports have been received so far, along with specific details about each interface. The default view shows the first router's interfaces alone. The remaining **routers'** interfaces are hidden. Click the **[Show All]** link to display all **routers'** interfaces on the Dashboard. Click the **[Hide All]** link to hide all interfaces and show only the router names in the Router List.

You can click on the device name and drilldown to see the particular device-based 10 top interfaces based on utilization and speed, top protocols, top application, top source, top destination, top conversation, top DSCP. You can export this particular device based report as pdf by clicking on the pdf icon on the right top.

You can set filters on the Dashboard view to display only those interfaces whose incoming or outgoing traffic values exceed a specified percentage value. Click the **[Filter]** link to specify minimum percentage values for IN or OUT traffic. Click the **Set** button for the changes to take effect. The filter settings are then displayed beside the **[Filter]** link. Click the  icon at any time to clear the filter settings and display all interfaces on the Dashboard again.





By clicking on the **Select Period**, the required time period for which the traffic details need to be seen can be selected from the drop-down. Reports corresponding to the chosen time period is shown in the Dashboard View.

The purpose of icons and buttons in the Router List is explained below.

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the interfaces corresponding to the router
	Click this icon to hide the interfaces corresponding to the router
 (before Router Name)	Click this icon to change the display name of the device, its SNMP community string, or its SNMP port. You can also choose to get the Interface Name details from one of 3 fields - IfDesc, IfName, or IfAlias.
 (before Interface Name)	Click this icon before the interface name to change the display name of the interface, or its link speed (in bps). You can also set the SNMP parameters of the router corresponding to an interface by clicking the link present in the <b>Note</b> included below the settings. You can also provide the V9 sampling rate for the particular interface (is "1" by default), which is taken into account for flow calculation.
 (near Refresh this page)	Click this icon, to set the time period for refreshing the page contents.
	Click this link to troubleshoot an interface. You can troubleshoot only <b>one</b> interface at a time. <b>Note:</b> Troubleshooting results are shown directly from raw data. Hence results depend on the raw data retention time period set in Settings
	Click this icon to see a quick report for the respective interface. This report shows you all the details about the traffic across that interface for the past one hour
	Indicates that NBAR report is available for the interface

The Interface Name column lists all the interfaces on a discovered device. Click on an interface to view the traffic details for that interface.

The Status column indicates the current status of that interface.

Icon	Description
	The Status of the interface is unknown and no flows have been received for the past 10 minutes. The interface is not responding to SNMP requests.
	The interface is responding to SNMP requests and the link is up, but no flows have been received for the past ten minutes.
	The link is up, and flows are being received.
	The interface is responding to SNMP requests and the link is down and no flows are being received.

The IN Traffic and OUT Traffic columns show the **utilization** of IN and OUT Traffic on the respective interfaces for the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic graph for that interface. Use the Custom Report link to generate custom reports. Set the value in Refresh this Page to inform the application how frequently the refresh has to be done to fetch the most recent data.

### IP Group List

A set of 4 IP groups have already been defined and have been named as

- Mail sites (eg. Gmail, Yahoo, )
- Social network sites (eg. Facebook, Twitter, MySpace)
- Sports sites (eg. Foxsports, Cricinfo)
- Video sites (eg. Youtube, hulu, FoxinteractiveMedia)

Users can also add/ remove other sites that they feel can under these predefined IP groups.

### Enabling SNMP V3

SNMP V3 is the latest version of the Simple Network Management Protocol by Cisco. With SNMP V3, data can be collected securely from SNMP devices without fear of the data being tampered with or corrupted and confidential information, for example, SNMP Set command packets that change a router's configuration, can be encrypted to prevent its contents from being exposed on the network.

For NetFlow Analyzer to be able to successfully poll the routers, users need to give the SNMP V3 credentials to NetFlow Analyzer.

In the "Interface view" tab, click on "set SNMP", which appears on the top left besides "router name".

1. In the pop-up that follows, you can select the "router name", for which you need to create / apply credentials, from the drop-down.

**Note:** Retrieve the interface name and speed using the following SNMP parameters.

**Set SNMP parameters**

Router Name :

Router IP :

SNMP Community :

SNMP Port :

Default Interface Name :

**Also retrieve the router name** (this may over-ride the router name set manually in NetFlow Analyzer)

**Enable SNMPV3** ?

2. Check the "Enable SNMP V3" box, and click on the "credential settings"
3. You can add a new credential or apply an already present credential from the credential list.

**V3 settings for:**

**Credential List** [Add New](#)

<input type="checkbox"/>	<b>Credential Name</b>	<b>Description</b>
<input type="checkbox"/>	toolkitnoauth	
<input type="checkbox"/>	Cisco2611	
<input type="checkbox"/>	CISCO2811	

4. To **add a new credential**, click on "add new".

**V3 settings for:**

**Credential Setting**

Credential Name :

Description :

User Name :

Context Name :  ?

**Authentication**

Protocol :

Password :

**Encryption**

Protocol :

Password :

5. Once the "credential setting" pops up, users can key in the credentials as per the following table.

Parameters	Description
Credential name	Users can name it as they find necessary
Description	Write a brief description for ease of understanding
Username	Same as the one set in the router
Context name	Same as the one set in the router
Authentication protocol	Same as the one set in the router
Authentication password	Same as the one set in the router
Encryption protocol	Same as the one set in the router
Encryption password	Same as the one set in the router

### SNMP V3 Security Models and Levels

Model	Level	Authentication	Encryption	What happens
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	AuthNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	AuthPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

For more details on SNMP V3, you can also view the Cisco site.

### More Reports

Click on More Reports to Compare Device(s) over various time period(s) and to Generate Report based on custom defined criterion.

### Compare Devices

Compare Devices feature lets the user Compare multiple devices for the same time period or Compare the same Device over different time periods. eg: Every Day Report, Every Hour Report, Every Week Report, Every Month Report.

Field	Purpose/Description
Report Type	The report type could be one of : <ul style="list-style-type: none"> <li>• Compare Multiple Devices over the same time period ( or)</li> <li>• Compare same device over different time periods</li> </ul> as the case may be.
Select Period	When the Report Type is chosen as - <i>Compare Multiple Devices over the same time period</i> , the available Periods are <i>Last Hour, Last 6 Hour, Today, Last 24 Hours, Yesterday, Last Week, Last Month, Last Quarter</i> or <i>Custom Selection</i> . Custom Selection lets one choose the time period for which one desires the report to be generated.  When the Report Type is chosen as - <i>Compare same device over different time periods</i> , the available Periods are <i>Every Day Report, Every Hour Report, Every Week Report, Every Month Report</i> .
Select Device(s)	This allows the user to select the device( if the same device is to be compared over various time periods) or the set of devices ( that are to be compared for a single time period). The Select Devices option allows the user to select the devices in terms of Interface or IP Group ( By default the top 10 interfaces or IP Group by utilization are chosen) which can be modified by clicking on the <b>Modify</b> button
Generate Report	The Generate Report invokes the report for the defined criteria.

Field	Purpose/Description
	<b>Report Options:</b> The Report Options could be chosen to be one of <ul style="list-style-type: none"> <li>• Show Speed</li> <li>• Show Utilization</li> </ul> Show Packets
Maximize	When the Generate Report option is invoked, the filter condition frame is minimized to offer a better view of the graph ( report ) without scrolling. The filter frame can be restored by using the Maximize button.
Minimize	The Minimize button can be used to minimize the Filter Frame for a better view of the report (graph) generated without scrolling


## Search Devices

The **Search** link lets you set criteria and view specific details about the traffic across the network on various interfaces. Data to generate this report is taken directly from aggregated data.

Upon clicking the Search link a pop-up with provision to Select Devices & set criteria comes up. In the pop-up window that opens up, click the **Select Devices** link to choose the interfaces on which the report should be generated.

Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:


- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **View per page** lets you choose how many results to display.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report. The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also sort the data displayed either by Number of packets or Bytes.

## Dashboard AS View

The **Autonomous System View** displays information on all the autonomous systems (AS) to which a router belongs, along with traffic details for each AS.






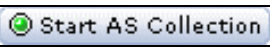

	In order to get AS info in this view, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.
---	---


The **Router List** displays each router along with the AS to which it belongs. Click on the AS Name to view the traffic report for that AS. The Dashboard also shows the organization to which the AS belongs, and the amount of incoming and outgoing traffic for the past one hour.

You can select the time period for which you need to see the AS data from the dropdown "Select Period".

The AS data can also be sorted as IN or OUT traffic. You can opt to see only the top n AS by selecting the relevant number from the dropdown.

The purpose of icons and buttons in the Router List are explained below.

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the autonomous systems to which this router belongs
	Click this icon to hide the AS corresponding to a router
	Click this icon before the router name to change the display name of the device, its SNMP community string, or its SNMP port
 (near Refresh this page)	Click this icon, to set the time period for refreshing the page contents.
	Click this icon to see the - Last 1 Hour report, on incoming and outgoing traffic for that AS for the past one hour
	Click this icon to start AS collection
	Click this icon to stop AS collection

Drilling down in to a particular AS gives an option to generate traffic report for the router comprising the AS by clicking on the "

## Google Map View

---

Google maps feature lets you physically locate your network resources on a map. This enables network administrators to have a feel of how distributed their network is and more importantly in a quick and easy drill down to resource-specific information. Information on up to 3 top interfaces linked to a router is shown in the map. NetFlow Analyzer, by using google maps, lets you position your devices on a map for a graphical presentation. You need to obtain a Google API Key in order to set up this. The steps to obtain one is elaborated below.

### Generating the Google Maps API key

The Google Maps API key is necessary to access the Google Map feature. You can get it by following the below steps:

- Click on the Google Map View tab - An alert message pops up which tells you the URL at which you can generate a key for your access
- Proceed to the **Configuring Google Map View** screen
- Follow **Step 1** - Click on the "**Click Here**" link
- A new window opens up which reads "Sign up for the Google Maps API".
  - Agree to the terms and conditions set forth in that page
- Specify the URL at which you will be accessing the application
- Click on the "Generate API Key" button
- A window will appear with the message " Your Key is" and the key below it
- Copy the key and paste it in the place provided in the application ( in **Step 2** )
- Click on "**Update**"

Once the key is pasted a map can be seen with the devices located on it. Refer to Settings to make any changes to the display.

Please note that, NetFlow Analyzer allows you to store only one key for a particular installation. In case you obtain the key using `http://<12.12.12.12>:8080` and try to access it using `http://<servername>:8080`, you will not be able to access the Google Map View and you may be prompted to obtain a fresh key. We recommend that you use the IP address / DNS name when you obtain the key and access NetFlow Analyzer using the same URL.

### Network layout in google map

You can visually see the devices that you are monitoring with NetFlow Analyzer on the google map and you can also see the traffic / interface details by clicking on the link. Given below are the steps to do so:

1. Click the "Configure network layout", on the top right, in the google map view
2. In the pop-up select the nodes (routers or switches). Provide the link name and description. Click "Next"
3. Select the interface relative to which you need to see the traffic details and "save".
4. Now you can see the traffic between the two link as per your need.

## IP Groups View

---

A set of 4 IP groups have already been defined and have been named as

- Mail sites (eg. Gmail, Yahoo, )
- Social network sites (eg. Facebook, Twitter, MySpace)
- Sports sites (eg. Foxsports, Cricinfo)
- Video sites (eg. Youtube, hulu, FoxinteractiveMedia)

Users can also add/ remove other sites that they feel can under these predefined IP groups by going to "Admin Operations" >>."IP Groups"


Information on IP groups created so far, is displayed below both the Global View tabs. This is also displayed when the **All Groups** link is clicked on the **IP Groups** pane on the left.


Initially when no IP groups have been created, you will simply see a status message "**No IP groups have been configured**".

The **IP Group List** shows all the IP groups that have been created so far. Click the **View Description** link to view descriptive information on all IP groups created. Alternatively you can click the **View Description** link against each IP group to view descriptive information on that IP group alone.

Click the IP Group name to view traffic graphs specific to that IP group. From the traffic graph, you can navigate to see the top applications, top hosts, and top conversations in this IP group.

The **IN Traffic** and **OUT Traffic** columns show the volume of incoming and outgoing traffic in the IP group generated over the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic report.

Click the  icon to see a consolidated traffic report for the respective IP group. This report shows you all the details about incoming and outgoing traffic in this IP group in a single report.

Click the  icon to see the speed graph for the particular IP group.

# Traffic Reports

## NetFlow Traffic Reports


---

NetFlow Analyzer generates traffic reports in real-time, as soon as NetFlow data is received from an interface.

The traffic reports in NetFlow Analyzer include information on:

- Traffic Trends
- Top Applications
- Top Hosts
- Top Conversations

Apart from these pre-defined reports, Search Report let you define criteria and generate specific reports on network activity. Consolidated Reports show you overall traffic statistics for an interface or AS as applicable. Troubleshooting Reports let you troubleshoot an interface using raw data directly.

Click the  icon or the **Troubleshoot** link in the page to troubleshoot this interface.


From any page, you can the export the report as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement.


## Real-time Traffic Graphs

NetFlow Analyzer generates traffic graphs as soon as Netflow data is received. The **Traffic** tab shows real-time traffic graphs for incoming and outgoing traffic. Depending on which link was clicked, you can see traffic graphs for an interface or IP group.

The graph and the data points can be viewed as 1 or 5 or 15 mins average by selecting from the top right.

Tabs above the traffic graph, let you view the graph in terms of volume of traffic, speed, link utilization, and number of packets received.


 The **Packets** tab shows the number of actual packets of traffic data received. This information is included in exported Netflow data.


You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.

The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this interface or IP group, for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

### Time Filters

The default graph is for the "Last Day". You can choose to see hour-based data in the traffic graphs for daily and weekly reports. To do this, first select the **Last Day Report** or **Last Week Report** option in the top time selection bar. When the respective traffic graph is displayed, the table below the graph includes the  icon next to the **Category** label.

Click the  icon to specify the hourly time interval for which you want to see traffic graphs. Click the **Show** button to set the filter and see hour-based values in the traffic graph as well as the table below. Click the **Reset** button to turn the filter off and switch to the regular traffic graphs.

### 95-th Percentile

The 95th percentile is the number that is greater than 95% of the numbers in a given set. The reason this statistic is so useful in measuring data throughput is that it gives a very accurate picture of the maximum traffic generated on an interface. This is a standard measure that is used for interpreting the performance data.

The 95th Percentile is the highest value left when the top 5% of a numerically sorted set of collected data is discarded. It is used as a measure of the peak value used when one discounts a fair amount for transitory spikes. This makes it markedly different from the average. The following example would help you understand it better.

Consider if the data collected for CPU Utilization is 60,45,43,21,56,89,76,32,22,10,12,14,23,35,45,43,23,23,43,23 (20 points). This list is sorted in descending order and a single top value, 89, is discarded. Since 1 constitutes 5% of 20, we discarded 1 value in this case. The highest value in the remaining list, 76, is the 95th percentile.

## Selectable Graph

NetFlow Analyzer brings you the added advantage of drill-down to the traffic graphs presented. As you hover the mouse over the plot-area you can see a "+" - cross-hair icon. Click on an area of the graph and holding the mouse down, drag it to the point(time period), you wish to further drill down to. For example : Having chosen a Last week report you could choose to study two specific days by selecting them. You could further drill down on until the time period you have chosen is more than 1 minute. The [Reset Graph](#) button take you to a time period depending on the time difference between the From time and the system time.

### Illustration


If you choose Last Hour Report at 18:15 hours, then a graph with a plot of data from 17:15 to 18:15 is shown. If you choose the time period 17: 25 to 17:50 then a corresponding graph with 1 Minute Average is shown. When you click on the [Reset Graph](#) button the screen changes to the Last Hour report. ( as the time difference between the From Time 17:25 and system time 18:20 is less than 1 hour)

Thus depending on the time difference you are either taken to the Last Hour or Last Day or Last Week or Last Month or Last Quarter graph.

## Top Applications

The **Applications** tab shows you the top applications and top protocols for the selected time period. The default view shows the **Top ApplicationIN Report**. This report shows the distribution of incoming traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between options available in the drop-down to view the particular application traffic. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.


The Show Ports Link next to an application name indicates that that application is not identified by NetFlow Analyzer. When you click on Show Ports Link, a window opens up showing the port and protocol details for this application. If it is a valid application you can then add it to the list of applications in the Application Mapping page.



The Show Ports Link will be displayed next to an unknown application only in the Last Hour report.

Click on an application's name to see the Top Conversations that contributed to this application's traffic.

The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each application. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can export as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement.

## Applications Group

Applications can be grouped together in NetFlow Analyzer and can be viewed as a single entity. To create applications group click one **"applications / QoS maps"** below **"Admin operations"** tab on the left side.

On the four tabs on top, click on **"Application groups"**. From here, you can add, modify or delete application groups.

To add application groups, click on **"Add"**. Mention an application group name and group description. After which, you can simply add the applications you want to group together, from the list of available applications listed there. And **"Save"** to view the application group.

## Viewing Top Protocols

Click on the **Protocol Distribution** link to see the top protocols for the selected interface or IP group, in a new window.

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.



This report sorts traffic based on the protocol used, while the **Application IN/OUT Report** sorts traffic based on the application, i.e., the combination of port and protocol.

Click on a protocol's name to see the Top Conversations that used this protocol. The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each protocol. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can export the report as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement.

## Source and Destination Tabs

In the source and destination tabs, you can view the source and destination IP addresses of the traffic. You can also categorize the IP addresses based on the region by clicking on the "Show Geo Locations" link.

For the **first time users**:

Click on the "show geo locations" link. Please download the file from the location provided in the pop-up and save it under 'NetFlow-Home' directory

## Top Hosts

---


The **Source** tab shows the top source hosts contributing to traffic in the selected time period. The default view shows the **Top SourceIN Report**.

The **Destination** tab shows the top destination hosts contributing to traffic in the selected time period. The default view shows the **Top DestinationIN Report**.

Choose between **IN** and **OUT** to display the top hosts in incoming or outgoing traffic.



When you drill down from an IP group, traffic is unidirectional, and hence the **IN** and **OUT** options are not available.

The Time Period box lets you choose between options available in the drop-down as per your requirement. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate source or destination traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.

Click the **Show Network** link to see the network-wise top sources and destinations.  
Ex: 192.168.4.0 / 24 . Here 192.168.4.0 is the IP address and 24 is the network mask.


The **Show** box above this table lets you choose how many hosts need to be displayed. You can set this value from the Settings page.

The pie chart below this report shows what percentage of bandwidth is being used by each host. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can export the report as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement.

## QoS

---

QoS or Quality of service is the most important factor that determines how effectively the available enterprise bandwidth is being used in the WAN. It is also an index of the overall User Experience of the available Bandwidth.

The QoS feature by default lists out the Top DSCP IN Report. Clicking on the Show Applications link lists out the various DSCP values along with the list of applications that comprise the DSCP. It also lists out details on Traffic and percentage utilization of the total traffic by each of the applications and the DSCP group as a whole. Clicking on the  icon next to the DSCP value gives a detailed traffic graph in a pop-up screen.

### DSCP

The DSCP Groups can be viewed by clicking on the View DSCP Group link. If no DSCP Groups have been created earlier, then an appropriate message is displayed and the user is prompted to create a DSCP group. The bottom of the page lists the Top DSCP IN Traffic as a Pie Distribution.

The time period for which the report is shown can be controlled by using the time selection bar at the top.

### TOS

Because the Internet by itself has no direct knowledge of optimizing the path for a particular application or user, the IP protocol provides a facility for upper layer protocols to convey hints to the Internet Layer about how the tradeoffs should be made for a particular packet. This facility is the "Type of Service" facility, abbreviated as the "TOS facility".

The TOS facility is one of the features of the Type of Service octet in the IP datagram header. The Type of Service octet consists of three fields. The first 3 bits (0,1,2) are for the first field, labeled "Precedence", intended to denote the importance or priority of the datagram. The second field, labeled "TOS", denotes how the network should make tradeoffs between throughput, delay, reliability, and cost. The last field, labeled "MBZ" (for "must be zero") above, is currently unused. The originator of a datagram sets this field to zero (unless participating in an Internet protocol experiment which makes use of that bit). Routers and recipients of datagrams ignore the value of this field. This field is copied on fragmentation.

#### Specification of the TOS Field

The semantics of the TOS field values (expressed as binary numbers):

<b>1000</b>	<b>minimize delay</b>
<b>0100</b>	<b>maximize throughput</b>
<b>0010</b>	<b>maximize reliability</b>
<b>0001</b>	<b>minimize monetary cost</b>
<b>0000</b>	<b>normal service</b>

The values used in the TOS field are referred to as "TOS values", and the value of the TOS field of an IP packet is referred to as the "requested TOS". The TOS field value 0000 is referred to "default TOS." Because this specification redefines TOS values to be integers rather than sets of bits, computing the logical OR of two TOS values is no longer meaningful. For example, it would be a serious error for a router to choose a low delay path for a packet whose requested TOS was 1110 simply because the router noted that the former "delay bit" was set.

Although the semantics of values other than the five listed above are not defined, they are perfectly legal TOS values, and hosts and routers must not preclude their use in any way. Only the default TOS is in any way special. A host or router need not make any distinction between TOS values

For example, setting the TOS field to 1000 (minimize delay) does not guarantee that the path taken by the datagram will have a delay that the user considers "low". The network will attempt to choose the lowest delay path available, based on its (often imperfect) information about path delay. The network will not discard the datagram simply because it believes that the delay of the available paths is "too high" (actually, the network manager can override this behavior through creative use of routing metrics, but this is strongly discouraged: setting the TOS field is intended to give better service when it is available, rather than to deny service when it is not).

### Use of the TOS Field in Routing

Both hosts and routers should consider the value of the TOS field of a datagram when choosing an appropriate path to get the datagram to its destination. The mechanisms for doing so are discussed in this section.

Whether a packet's TOS value actually affects the path it takes inside a particular routing domain, is a choice made by the routing domain's network manager. In many routing domains the paths are sufficiently homogeneous in nature that there is no reason for routers to choose different paths based up the TOS field in a datagram. Inside such a routing domain, the network manager may choose to limit the size of the routing database and of routing protocol updates by only defining routes for the default (0000) TOS.

Neither hosts nor routers should need to have any explicit knowledge of whether TOS affects routing in the local routing domain.

### Inherent Limitations:

The most important of all the inherent limitations is that the TOS facility is strictly an advisory mechanism. It is not an appropriate mechanism for requesting service guarantees. There are two reasons why this is so:


- Not all networks will consider the value of the TOS field when deciding how to handle and route packets. Partly this is a transition issue: there will be a (probably lengthy) period when some networks will use equipment that predates this specification. Even long term, many networks will not be able to provide better service by considering the value of the TOS field. For example, the best path through a network composed of a homogeneous collection of interconnected LANs is probably the same for any possible TOS value. Inside such a network, it would make little sense to require routers and routing protocols to do the extra work needed to consider the value of the TOS field when forwarding packets.
- The TOS mechanism is not powerful enough to allow an application to quantify the level of service it desires. For example, an application may use the TOS field to request that the network choose a path which maximizes throughput, but cannot use that mechanism to say that it needs or wants a particular number of kilobytes or megabytes per second. Because the network cannot know what the application requires, it would be inappropriate for the network to decide to discard a packet which requested maximal throughput because no "high throughput" path was available.

## Top Conversations

---

The **Conversation** tab shows the top conversations contributing to traffic in the selected time period.


Choose between **IN** and **OUT** to display the top conversations in incoming or outgoing traffic.

The Time Period box lets you choose between options available in the drop-down as per your requirement. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate conversation traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names.

The **Show** box above this table lets you choose how many conversations need to be displayed. You can set this value from the Settings page.

The **Group by** box lets you group conversations by source, destination, or application. The default list shows the conversations sorted in descending order of number of bytes of traffic.


The pie charts below this report show the top sources, destinations, and conversations contributing to traffic for the selected time period. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can export the report as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement.

## AS Traffic Reports

---

The Traffic report for autonomous systems shows the amount of incoming and outgoing traffic for that AS, over the past one hour.

Tabs above the traffic graph let you view the graph in terms of volume of traffic, speed, and number of packets received.

You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.


The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this AS for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

## Troubleshooting


---

The **Troubleshoot** link lets you set criteria and view specific details about the traffic across a single interface. Data for Troubleshooting reports is taken directly from raw data. Which means that Troubleshooting reports will be available only for the maximum time period for retaining raw data, configured under Settings.

Click the  icon against an interface on the Dashboard Interface View, or the **Troubleshoot** link present above the traffic graphs for an interface, to open a popup with options to set criteria for viewing reports. In the pop-up window that opens up, click the **Select Devices** link to change the interface that you want to troubleshoot.


Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Ensure that the time period selected, falls within the Raw Data Retention Period set under Settings, otherwise graphs will show no data.

Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.


Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the  icon or the **Print** link.

## Consolidated Reports


---

Consolidated reports let you see all the traffic details for an interface or IP group at one glance. You can then print this report or save it as a PDF file.

Click the **Consolidated Report** link to see all traffic details for an interface at one glance. The same report can be accessed from the Global Dashboard when the  icon against an interface or IP group is clicked.

The Custom Selection box lets you select different time periods for the traffic data.

- The **1 Hour Report** and **1 Day Report** options show you traffic details over the past one hour and one day respectively.
- The **8AM to 8PM** option shows you traffic details from 8 a.m. to 8 p.m. of the previous day. This is a peak hour report, based on the normal working hours of an enterprise.

Apart from these options, the **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Once you select the desired time period, click the **Show Report** button to display the corresponding consolidated report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names. From here, you can the export as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement, or print it by clicking the Print icon.

## Compare Report - NetFlow Analyzer Global Report

### Compare Devices


Compare Devices feature lets the user Compare multiple devices for the same time period or Compare the same Device over different time periods. eg: Every Day Report, Every Hour Report, Every Week Report, Every Month Report.

Field	Purpose/Description
Report Type	The report type could be one of : <ul style="list-style-type: none"> <li>• Compare Multiple Devices over the same time period ( or)</li> <li>• Compare same device over different time periods</li> </ul> as the case may be.
Select Period	When the Report Type is chosen as - <i>Compare Multiple Devices over the same time period</i> , the available Periods are <i>Last Hour, Last 6 Hour, Today, Last 24 Hours, Yesterday, Last Week, Last Month, Last Quarter</i> or <i>Custom Selection</i> . Custom Selection lets one choose the time period for which one desires the report to be generated.  When the Report Type is chosen as - <i>Compare same device over different time periods</i> , the available Periods are <i>Every Day Report, Every Hour Report, Every Week Report, Every Month Report</i> .
Select Device(s)	This allows the user to select the device( if the same device is to be compared over various time periods) or the set of devices ( that are to be compared for a single time period). The Select Devices option allows the user to select the devices in terms of Interface or IP Group ( By default the top 10 interfaces or IP Group by utilization are chosen) which can be modified by clicking on the <b>Modify</b> button
Generate Report	The Generate Report invokes the report for the defined criteria.  <b>Report Options:</b> The Report Options could be chosen to be one of <ul style="list-style-type: none"> <li>• Show Speed</li> <li>• Show Utilization</li> </ul> Show Packets
Maximize	When the Generate Report option is invoked, the filter condition frame is minimized to offer a better view of the graph ( report ) without scrolling. The filter frame can be restored by using the Maximize button.
Minimize	The Minimize button can be used to minimize the Filter Frame for a better view of the report (graph) generated without scrolling

## Search Report


---

Custom Reports let you set several criteria and view specific reports. This is especially useful in finding out the bandwidth utilization of a specific host or application. Custom reports can also tell you details about a certain application and which hosts are using it, thereby helping to troubleshoot, and even detect virus activities.


Click the  icon or the **Custom Report** link on the Dashboard to set criteria and view custom reports. In the pop-up window that opens up, click the **Select Devices** link to select the routers and/or interfaces whose traffic needs to be analyzed.

Under Report Criteria, you can specify a maximum of three filtering criteria:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report. The report can be exported as csv also.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the  icon or the **Print** link.



Custom Reports are different from Troubleshooting Reports. You can troubleshoot only **one** interface at a time, whereas Custom Reports can be generated across interfaces. Data for Troubleshooting reports is taken directly from raw data, whose maximum retention period can be set from Settings. But data for Custom Reports is taken from aggregated data in the database.

## Admin Operations

---

NetFlow Analyzer lets you perform many administrative tasks typical of an enterprise network administrator, such as managing a group of routers, handling different users, setting up alerts, etc.

Explore the following sections to know more about the administrative options available in NetFlow Analyzer.

Setting	Description
Billing	Allows you to Add/Edit bill plans, View reports
Product Settings	Click this link to change default server settings for NetFlow Analyzer and also set up the mail server for sending e-mail notifications
Application Mapping	Click this link to configure applications based on port-protocol combinations
IP Group Management	Click this link to create IP groups that let you view traffic details for a selected group of devices, applications, or interfaces
Alert Profiles Management	Click this link to add new alert profiles or modify existing ones
Scheduler Configuration	Allows setting of time intervals at which network traffic reports are generated automatically and mailed to desired recipient(s)
Device Group Management	Click this link to set up device groups based on devices exporting NetFlow data to NetFlow Analyzer
NBAR/ CBQoS	Click this link to learn how to configure your device for NBAR and CBQoS
User Management	Click this link to create different users for logging in to NetFlow Analyzer and assign access privileges to each user
License Management	Click this link to manage the list of devices exporting NetFlow data to NetFlow Analyzer based on the current license applied
Change Password	Click this link to change your own password for logging in to NetFlow Analyzer

## Product Settings

The Settings option includes several server configuration settings that you can configure from the user interface namely :

- Server Settings
- Advanced Settings
- Storage Settings
- Mail Server /Proxy Server Settings
- Google Map Settings

### Server Settings

#### Server Settings

The Server Settings option includes several configuration settings that you can configure from the user interface

Option	Default Value	Requires server restart	Description
NetFlow / sFlow Listener Port	9996	yes	The port on which NetFlow Analyzer listens for NetFlow exports. You need to configure devices to send NetFlow exports to this port. In case you are exporting NetFlow from multiple routers, please configure multiple listener ports. You can specify upto 5 listener ports, each separated by a comma. You will need to restart the NetFlow Analyzer server when you change the listener port
Webserver Port	8080	yes	The port used to access NetFlow Analyzer from a web browser
Record Count	100	no	This number governs the top N conversations that are retained for every 10 minute interval for each interface. Set it to 100 for maximum visibility into your traffic. The default record count is 100 but the minimum number of records that can be kept in the database for all traffic data is 10. This is also the maximum value that can be selected from the <b>Show</b> box in all traffic reports

#### DNS Settings

Option	Description
Resolving DNS Names	DNS names may be resolved only when "Resolve DNS" is clicked or automatically by default
DNS count in cache	The DNS count could take any value from 5000, 7500 and 10,000
User Defined DNS names	User defined DNS names can be entered or modified. This value will over-ride the system resolved DNS value.
Clear DNS Cache	Clicking on this button will clear all DNS entries that have been resolved by the system. The application asks for a confirmation before initiating the clearing action

## Advanced Settings

The Advanced Settings option includes the Flow Filter Settings and the Radius Server Settings and their corresponding configuration settings.

### Flow Filter Settings

The Flow Filter settings empower the administrator with the option to

- exclude ESP\_App on user defined interfaces - This helps in ensuring that traffic is not double counted in case of ESP tunnels.
- suppress Access Control List related drops (based on destination interface being null) on user defined interfaces.
- suppress output interface accounting on user defined interfaces - Useful when working with WAN accelerator.
- apply GRE filter on the cryptomap tunnels to prevent double counting of GRE traffic.

Option	Description
Select edge interfaces of a cryptomap tunnel to apply ESP application filter	One could add or modify interfaces to apply the ESP application filter. Enabling NetFlow on cryptomap tunnel interfaces double counts the ESP traffic. To prevent this please apply this filter on cryptomap tunnel interfaces. It is possible to add or modify interfaces.
Select interfaces to apply access control traffic filter	Access control filter drops the flow information which contains data pertaining to dropped traffic due to Access Control List. Please apply this filter to drop such flows. These flows have the destination interface as null. If any interface is selected to apply this filter, all the traffic coming from this interface with destination as null interface will be dropped.
Select interfaces to apply output interface suppression filter	Please select any WAN optimizer's LAN facing interfaces to suppress the incorrect out traffic ( due to compression ) reported by them. This filter stops the out traffic for any interface that is coming as a destination interface of a flow for a selected interface. When a WAN optimizer sends a flow which has source and destination interfaces as A and B respectively , if you select interface A to perform output suppression, B will not get out traffic which is not a correct traffic if reported by interface A ( since compression is happening on interface B on the WAN optimizer )
Select edge interfaces of a cryptomap tunnel to apply GRE application filter	Please select any cryptomap tunnel interface in which you want to apply GRE filter. This prevents the GRE traffic getting double counted. Otherwise the cryptomap interface in which NetFlow is enabled double counts the GRE traffic.

### Radius Server Settings

Radius Server ( Remote Authentication Dial In User Service ) is an AAA (Authentication, Authorization and Accounting ) protocol for controlling access to resources in a network. Radius Server is useful in centralised management of user credential details. It facilitates a single global set of credentials that are usable on many public networks. Once the user roles are defined in the User Management feature of NetFlow Analyzer subsequent handling of the user profiles can be done from the Radius Server.

<b>Option</b>	<b>Description</b>
Radius Server IP	The IP address of the Radius Server where credentials are configured
Radius Server Authentication Port	The authentication port of the Radius Server
Radius Server Protocol	The Radius Server Protocol could be any of PAP, CHAP, MSCHAP, MSCHAP2
Radius Server Secret	The Secret refers to the password that is necessary to access the Radius Server
Authentication Retries	Authentication Retries can take one of the values from 1, 3, 5. This defines the number of times authentication attempt is allowed

## Storage Settings

---

### NetFlow Raw Data Settings

NetFlow Analyzer classifies data into 2 types namely Aggregated Data and the Raw Data.

Aggregated Data represents the total IN and OUT traffic, the top 100 application and the top 100 conversation for each interface for every 10 minute intervals. Data is progressively stored in 10 minute, 1 hour, 6 hour, 24 hour and weekly data points for older data - the most recent data is available with 10 minute granularity and data older than 90 days is available in weekly granularity.

This mechanism of storing the top 100 is done to ensure that the database does not grow infinitely. The amount of hard disk space required to store the aggregated data forever is about 150 MB per interface.

In addition to the aggregated data, NetFlow Analyzer 5 allows you to store all raw netflow data for up to 1 month. The time period for which you can store this raw data (Raw Data Period) depends on the number of flows received by NetFlow Analyzer and the amount of free disk space available on your computer. Each flow is about 60 bytes. Troubleshooting and Alert reports are generated from Raw data since it provides high level of granularity.

NetFlow Analyzer indicates the flows received per second in the Raw Data Settings tab on the Settings link. You should set the raw data period ( **Retain Raw Data** ) based on the calculation below:

$$\text{Raw Data Period (in hours)} = \frac{\text{Free hard disk space} - (150 \text{ MB} * \text{No. of Managed Interfaces})}{60 \text{ Bytes} * 3600 \text{ seconds} * \text{Flows Per Second}}$$

You can use the recommendation provided by the software to set your Raw data storage period. The maximum raw data storage period is 1 month and the minimum is a day. Similar to the alerting feature, you can choose to have a mail sent whenever the disk space is less than a threshold value( This is set as a percentage value). In addition you can specify the free disk space threshold below which old raw data will be cleared up. This could be as percentage value of the total disk space. This can also take on the value of "Never", in which case the disk place is not cleared up at all.

### One minute Data-Storage Settings

To set the period for which one minute flow data has to be stored use the **Retain One Minute Data** option. You could choose one of 1 month, 3 months, 6 months or 1 year. You will require a free disk space of 2MB to store one month of one minute traffic data for a single interface. The default period is 3 Months.

### NBAR Data-Storage Settings

You can use this option to specify the time period for which NBAR data has to be retained. You could retain the NBAR data a minimum of 1 day or a maximum of 1 year. You will require a free disk space of 30 MB in order to store NBAR data for a month for each interface. The default value is 2 months.

Click on the "Update" button for the settings to take effect.

## Mail Server / Proxy Server Settings

### Mail server settings

These settings are important when e-mail notifications have to be sent for alerts generated and when Scheduled Reports have to be emailed

Option	Default Value	Description
Outgoing SMTP Server	smtp	The name of the outgoing SMTP server used to send e-mails
Port	25	The port number on the outgoing server that is used to send e-mails
Default e-mail address to send alerts	(optional)	The default e-mail address to which e-mail notifications have to be sent. Separate multiple e-mail addresses by a comma (.). This is mandatory.
From Address	(optional)	The "From" address of the mail that is being sent. This is optional.
Requires authentication	unchecked	Select this checkbox if the mail server needs authentication
User Name	(optional)	The authentication user name for the mail server
Password	(optional)	The corresponding password for mail server authentication

## Google Map Settings

Google maps feature lets you physically locate your network resources on a map. This enables network administrators to have a feel of how distributed their network is and more importantly for quick and easier drill down to resource-specific information. Information on up to 3 top interfaces linked to a router is shown in the map. The Google Map settings lists all the devices and their corresponding location. This page gives you the option to place each of the devices in their respective locations

### Assigning a location to a router

Clicking on the **Assign** link opens up the Google map. Follow the instructions below to place a device on the map:

1. Click on the location to place the device on the map. Use the controls on the top left to navigate or zoom
2. You will see an image indicating your selection
3. To change the location click on the image, it will vanish and then select a new location
4. Enter the location in the 'Location Name' field and hit "Save location"

Now a location has been assigned to a router.

### Editing a location

To edit a specific location on the map, click on the "Edit" link under the Google Map Settings tab. Now the map view will open up with the location you had last specified. To edit it ( to move the pointer to the desired location) click on the area of the map where you think it should point to. The last location you spot(click) in the course of locating your resource through "n" different clicks on the map is taken as the final.

### Deleting a location

You may remove any resource/ router from being shown on the map by clicking on the delete button against the resource in the Google Map Settings tab.

## Application Mapping, Application Group, DSCP Mapping and DSCP Group

### Application Mapping

The **Application Mapping** option lets you configure the applications identified by NetFlow Analyzer. You can add new applications, modify existing ones, or delete them. Please see the Additional Notes on Application Mapping section to understand this feature more clearly. Also it is possible to associate an IP address with an application.

### Adding an Application

Follow the steps below to add a new application:

1. Click the **Add** button to add a new application
2. Enter the port number of the new application. To enter a port range, separate the start and end points of the range with a hyphen. (eg.) 1400-1700
3. Choose the protocol from the list of protocols
4. Choose one of the options from IP Address / IP Network / IP Range. Depending on what you opt a set of fields are enabled and should be filled.
  - If you opt for **IP Address** then you have to enter the address in the IP Address box.
  - If you opt for **IP Network** then you have to enter the IP Network and IP Netmask details.
  - If you opt for **IP Range** then you have to enter the Start IP, End IP and IP Netmask Enter a unique name for the application
5. The Application Name has to be entered finally by which the IP address is associated with an application.



Ensure that the combination of port number and protocol is unique. If not, the older application mapping will be deleted.

Once you are done, click the **Update** button to save your changes.

### Modifying an Application

Select an application and click the **Modify** button to modify its properties



You can only change the name of the application. If you need to change the port or the protocol, you have to delete the application, and add it as a new application.

Once you are done, click the **Update** button to save your changes.

### Deleting an Application

Select an application and click the **Delete** button to delete it. The application is permanently deleted, the corresponding port is freed, and can be assigned to another application

### Additional Notes on Application Mapping

Applications are categorized based on the source address, destination address, source port, destination port and protocol values in the flow record. These values are matched with the list of applications in the Application Mapping.

The check is done first with the smaller of the 2 ports (source port / destination port), and if no match is found the bigger of the 2 ports is mapped

Application mappings created with specific IP address / IP Range / IP Network is given higher priority over applications mappings with no IP address. For example assume you have 2 application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	10.10.1.0( 255.255.255.0)	APP1
80	TCP	Any	APP2

If a flow is received with source address 10.10.10.10 and Port as TCP-80 then it is classified as APP1. Only TCP-80 flows from non-10.10.10.0 network will be classified as APP2.

Application mappings created with single port is given higher priority over applications mappings with port range. For example assume you have application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	any	APP1
70 - to - 90	TCP	any	APP2

If a flow is received with Port as TCP-80 then it is classified as APP1.

Applications are categorized based on the source address, destination address, source port, destination port and protocol values in the flow record.

The smaller of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list.

If no match is found, the smaller of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the application is categorized as protocol\_App (as in TCP\_App or UDP\_App)

In case the protocol is not available in the application mapping list, the application is categorized as Unknown\_App

The sequence in which the mappings are checked is as follows:

1. Application mapping with specific IP address / IP Range / IP Network is matched.
2. Application mapping with no IP address and single port number / port range.

### Application Group

Application Groups allow you to define your own class of applications by including one or more applications. For example, you might want to classify all your database applications like Oracle, MySql, MS-Sql in to one group called the DataBase group. Initially when no application groups have been created a message to that effect is displayed. The Application Group report can be viewed on the Application tab for each interface.

## Adding an Application Group

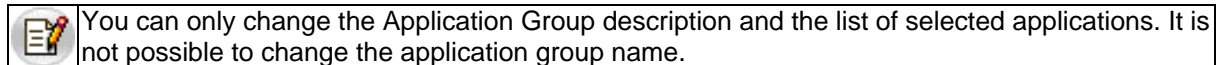
Follow the steps below to add a new application group:

1. Click the **Add** button to proceed to the Add Group Screen
2. Enter the Group Name and the Group Description (eg.) DataBase Group - Contains the Oracle DB and MySql DB
3. Choose the applications from the list of applications in the left pane
  - Select an application by clicking on it.
  - Use the " >> " button to include the selected application to the right pane - "Selected Applications" list.
  - Add as many applications as you want to this group.
4. Click on update for the application group to be created with the list of applications you had selected.

You may create additional Application Groups by clicking on the Add button and following the above steps.

## Modifying an Application Group

Select the Application Group you wish to modify and click on the "Modify" button.



Once you are done, click the **Save** button to save your changes.

## Deleting an Application Group

Select the application group you want to delete and click on the "Delete" button. You are asked for a confirmation to delete and if you confirm the group is deleted.

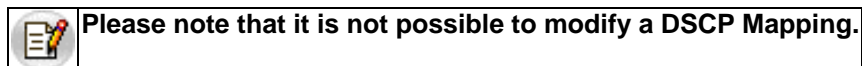
## DSCP Mapping

The DiffServ model for DSCP Mapping was developed to differentiate IP traffic so that the traffic's relative priority could be determined on a per-hop basis. Using DSCP Mapping you can name the DiffServ code points and monitor their traffic in troubleshooting reports under the DSCP tab. Note that the DSCP reports can be viewed on the Troubleshooting page by clicking on the DSCP tab.

## Adding a new DSCP Mapping

Click on the Add button to create a new DSCP Mapping. A window pops out where you may enter the Group Name and the Code Point ( a six-digit Binary Number). *For Example:* Data Centre devices - 001001. Click on the "Add" button to add this mapping.

## Modifying a DSCP Mapping



## Deleting a DSCP Mapping

Select the DSCP Mapping ( the combination of QoS Group Name and Code Points) you want to delete and click on the Delete button.

## DSCP Group

Quality of Service is used to measure, improve and guarantee transmission rates, error rates and other characteristics in a network setting. The DiffServ model for DSCP Mapping was developed to differentiate IP traffic so that the traffic's relative priority could be determined on a per-hop basis. Using DSCP Mapping you can name the DiffServ code points and monitor their traffic in troubleshooting reports under the DSCP tab. Note that the DSCP reports can be viewed on the Troubleshooting page by clicking on the DSCP tab. The DSCP group is very valuable in the deployment of QoS.

### Adding a new DSCP Group


Follow the steps below to add a new application group:

1. Click the **Add** button to proceed to the Add Group Screen
2. Enter the Group Name and the Group Description (eg.) DataBase Group - Contains the Oracle DB and MySQL DB
3. Choose the DSCP Names from the list of names in the left pane
  - Select a name by clicking on it.
  - Use the " >> " button to include the selected DSCP Name to the right pane - "Selected DSCP Names" list.
  - Add as many DSCP Names as you want to this group.
4. Click on Save for the DSCP Group to be created with the list of DSCP Names you had selected.

You may create additional DSCP Group by clicking on the Add button and following the above steps.

### Modifying a DSCP Group

Select the DSCP Group you wish to modify and click on the "Modify" button.

	You can only change the Group description and the list of selected applications. It is not possible to change the DSCP group name.
---	--

Once you are done, click the **Save** button to save your changes.

### Deleting a DSCP Group

Select the DSCP Group you want to delete and click on the Delete button.

## IP Group Management

---

A set of 4 IP groups have already been defined and have been named as

- Mail sites (eg. Gmail, Yahoo, )
- Social network sites (eg. Facebook, Twitter, MySpace)
- Sports sites (eg. Foxsports, Cricinfo)
- Video sites (eg. Youtube, hulu, FoxinteractiveMedia)

Users can also add/ remove other sites that they feel can under these predefined IP groups.

The IP groups feature lets you monitor departmental, intranet or application traffic exclusively. You can create IP groups based on IP addresses and/or a combination of port and protocol. You can even choose to monitor traffic from specific interfaces across different routers. After creating an IP group, you can view the top applications, top protocols, top hosts, and top conversations in this IP group alone.

This section will help you understand IP Groups and walk you through the steps needed to create and later delete an IP group if needed.

- Understanding IP Groups
- Defining an IP Group
- Operations on IP Groups
- Bulk Loading of IP Groups

### Understanding IP Groups

To further understand how the IP grouping feature can help in understanding exclusive bandwidth usage, consider the following two scenarios:

#### *Enterprise Network Scenario*

A typical enterprise setup where the main servers and databases are located at a central office, and all branch offices are given appropriate access privileges to these servers.

**Problem:** You need to track bandwidth used by each branch office while accessing an ERP/CRM application

**Solution:** Create an IP group for each branch office, along with the port and protocol of the ERP/CRM application running in the central office.

The traffic reports for each IP group will then show details on bandwidth used by the branch office while working with the ERP/CRM application. This information is very useful during traffic accounting and usage-based billing.

**End Note:** If the IP addresses in the branch offices are NATed (network address translated) by the web server, you can view overall bandwidth usage for the branch office, but not that of individual hosts within the IP group.

#### *Campus Network Scenario*

A typical campus network with several departments. Here IP addresses are usually not NATed by the web server.

**Problem:** You need to analyze bandwidth used by each department

**Solution:** Create an IP group for each department (IP address or address ranges), without specifying any port/protocol values.

The traffic reports for each IP group will then show bandwidth usage by that department along with information on top talkers, and top conversations within that department.

### Defining IP Groups

IP groups can be defined based on IP address and/or port-protocol combinations. In addition, you can filter IP group traffic based on interfaces. The following matrix shows the different combinations possible, along with a typical example usage for each combination.

Combination	IP Address	Port/Protocol	Interfaces	DSCP
IP Address	View bandwidth details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View bandwidth details across multiple interfaces, for a range of IP addresses.	View bandwidth details of the applications using a particular DSCP name
Port/Protocol	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across the network	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.	View web traffic using the particular DSCP name
Interfaces	View bandwidth details across multiple interfaces, for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.	[ Not possible ]	View the traffic traversing through the multiple interfaces with the particular DSCP name
DSCP	View bandwidth details of the applications using a particular DSCP name	View web traffic using the particular DSCP name	View the traffic traversing through the multiple interfaces with the particular DSCP name	[ Not possible ]

### Creating an IP Group

The **IP Group Management** link in the **Admin Operations** box lets you create, modify, and delete IP groups. Click this link, and then click **Create** to create a new IP group. Fill in the following information and click **Add** to add the new IP group to the current list of IP groups.

Field	Description
<b>IP Group Name</b>	Enter a unique name to identify this IP group
<b>IP Group Description</b>	Enter descriptive information for this IP group to help other operators understand why it was created.
<b>IP Group Based on</b>	Select whether you want to define this IP group based on IP address, DSCP names or port-protocol or the combination of any of the three.
<b>Specify IP/IP Range/Network</b>	Select the IP address, address range, or network that this IP group is based on. Use the <b>Add More</b> option to add additional specifications.
<b>Include/Exclude/ Between sites</b>	Include option includes the particular the IP address, address range, or network. Exclude option excludes the particular the IP address, address range, or network. Between sites option allows you to group the traffic between sites, which can be defined by two networks or IP addresses.
<b>Filter based on DSCP names</b>	Allows you to set filters based on the DSCP names of the applications.
<b>Associated Interfaces</b>	If you need to filter this IP group further, based on devices or different interface combinations, click the <b>"Select Devices"</b> link and select the different devices and interfaces whose traffic needs to be included in this IP group.
<b>IP Group Speed</b>	Enter the interface speed (in bits per second) for calculating percentage of traffic for this IP group.



If you add a new combination of ports and protocol, a popup opens stating that this combination of ports and protocol has not been mapped to any application. Add the combination as a new application in the same popup, and click **Update** to update the Application Mapping list with the new application.

## Managing IP Groups

Click the **IP Group Management** link in the **Admin Operations** box to view the list of IP groups created so far. The current status of the IP Group is also shown as **Enabled** or **Disabled**. Select the IP group that you want to modify, and click the **Modify** button to edit its settings. Once you are done, click **Add** to save and activate the new changes. To change a IP group's status from Enabled to Disabled or vice-versa click on the current status of the IP Group. It is possible to Enable or Disable all the IP Groups at once by using the "Enable All" and "Disable All" buttons.

To delete an IP group, select the IP group and click the **Delete** button. Deleting an IP group removes the IP group from the list of IP groups managed. All users assigned to this IP group will not see this IP group listed on their Dashboard.



Unmanaging an IP group will lead to bill generation for the particular IP group, **IF** that IP group has been selected for billing.

## Bulk loading IP Groups

NetFlow Analyzer allows bulk loading of IP group using the XML file(ipGroup.xml) contained in the location: **AdventNet\ME\NetFlow\troubleshooting**. using this file it is possible to define multiple IP groups at once. A sample configuration code looks like:

```
<IPGroups ip_group_name="Engineering" ip_group_desc="description in detail"
ip_group_speed="1000000">
  <GrpIPAddress addr_id="12.12.12.12" flag="include"/>
  <GrpIPNetwork netmask_addr_id="255.255.255.0" network_addr_id="12.12.13.0" flag="include"/>
  <GrpIPRange netmask_addr_id="255.255.255.0" start_addr_id="12.12.14.1"
end_addr_id="12.12.14.100" flag="exclude"/>
  <ApplicationNames port="80" protocol="TCP"/>
  <Selected_Devices>
  <Router Router_Name="192.168.111.113">
  <Interface interface_name="IfIndex1" />
  <Interface interface_name="IfIndex3" />
  </Router>
  </Selected_Devices>
</IPGroups>
```

Within this configuration it is possible to have any number of **GrpIPAddress** or **GrpIPNetwork** or **GrpIPRange** or **ApplicationNames** with Interface selection.

It is also possible to add specific criteria/exceptions to the group definition such as:

- configuring an IP group with just one network
- configuring an IP group with just one address
- configuring an IP group with just one range
- configuring an IP group with just port and protocol

- The user has to ensure that an IP group with the same name does not already exist and that the IP group name does not exceed 50 characters.
- If all the IP groups are loaded successfully, you can see the message "All ipgroups are successfully loaded" in the User Interface. If you try to load the same IP groups twice, you can see the message "Error in loading. IPGroup with name ':grp1' Already exists." in the User Interface. If there is no such file in the directory, you can see the message "NETFLOW\_HOME\troubleshooting\ipGroup.xml is not found." in the User Interface.
- After adding the IP group(s) it is possible to selectively include/exclude a IP Network/ IP Address/ IP Range from the user interface of the product.

## Alert Profiles Management



An alert profile is created to set the thresholds for generating alerts. The parameters to be set for creating an alert profile are;

- **Interfaces/ IP Groups / Interface Group** - The list of interfaces/ IP Groups / Interface Group whose bandwidth utilization must be watched
- **Traffic pattern** - The traffic to be watched - In Traffic, Out Traffic or a Combination of both
- **Application / Port(s)** - You can watch the traffic through all the applications or from a particular application. Similarly, through a single port or a range of ports
- **Threshold Settings** - It has 3 settings namely % utilization, no. of times, and duration.
  - **% Utilization** - When the utilization exceeds this limit, it is noted
  - **No. of time** - The number of times the utilization can be allowed to exceed the threshold before an alert is raised
  - **Duration** - The time period within which, if the threshold is exceeded the specified number of times - an alert is created(generated)

Netflow Analyzer calculates the bandwidth utilization of the specified interfaces/ IP Groups / Interface Group every minute. If the utilization exceeds the threshold value, the time when it exceeded is noted. Subsequently when it exceeds, the corresponding times are noted. If the number of times the utilization exceeds the specified limit, in the specified time duration, an alert is generated. When an alert is generated, you can also send an email to one / more people or send an SNMP trap to a manager application.

The **Alert Profile Management** option lets you create new alert profiles and manage existing ones (Modify or Delete). The Alert Profiles page lists all existing alert profiles, along with the number of alerts generated for each profile. The application comes loaded with a preconfigured alert that can trigger an email alert when a link goes down or when there are no flows for more than 15 minutes.

The various columns displayed in the Alert Profiles page are described in the table below:

Column	Description
Name	The name of the alert profile when it was created. Click on the alert profile's name to see more information about the alert profile.
Description	Descriptive information entered for this alert profile to help other operators understand why it was created.
Category	The category defines, to what type of alert an alert profile belongs to. The pre-loaded and pre-configured "Link Down" alert belongs to the "Link Status" category. All other alerts created by the user fall under the "Utilization"category.
Status (Enabled/Disabled)	This lists whether an alert profile is currently enabled or disabled. Click the  <b>Enabled</b> icon to disable an alert profile. When this is done, alerts will no longer be generated for that alert profile. Click the  <b>Disabled</b> icon to enable the alert. The Link Status alert becomes enabled only after the mail server settings have been set.
Last Hour Alerts	Lists the number of alerts generated for this alert profile in the last one hour. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
All Alerts	Lists the total number of alerts generated for this alert profile. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
Clear	Click the icon to clear all alerts generated for this alert profile

## Alerts List

The Alerts List is displayed when you click on any color against an alert profile in the Alert Profiles page, or from any link in the **Generated Alerts** box on the left pane. The list shows the alerts that were generated with the respective severity, along with the device that generated the alert, the time the alert was generated, and an option to view more details about the alert.

Click the **Details** link in the View column against an alert to view detailed information about the alert. The pop-up that opens up, shows the traffic graph outlining traffic values ten minutes before and after the alert was generated, along with details on top applications, sources, destinations, and conversations recorded during that time interval.

## Link Down Alert

This is a preconfigured alert to send an email when the link goes down or when there are no flows for more than 15 minutes. By default this profile is disabled. This is similar to other alerts that are manually configured except that it can't be deleted. It is possible to have emails sent by this alert whenever no flows are received for over 15 minutes. It becomes activated only after the mail server settings are configured.

## Operations on Alert Profiles

You can create new alert profiles, modify, or delete existing ones from the Alert Profiles page.

## Creating a new Alert Profile

	<b>Remember to set the active timeout value on the router to 1 minute so that alerts are generated correctly. Refer the Cisco commands section for more information on router settings.</b>
---	---

The steps to create an Alert Profile are:

1. Login to the NetFlow Analyzer client and click "**Alert Profile Management**" under "**Admin Operations**" in the left panel
2. Click "**Add**" to add a new Alert Profile
3. Fill in the following details

Field	Description
Alert Profile Name	Enter a unique name to identify this alert profile
Description	Enter descriptive information for this alert profile to help other operators understand why it was created.
Select Source	By default all Interfaces / IP Groups/ Interface Group sending NetFlow exports are selected. If you want this alert profile to apply to certain interfaces/ ip groups / Interface Groups only, click the <b>Modify Selection</b> link. In the pop-up window, select the required devices and interfaces or select the IP Group Names and click <b>Update</b> to save your changes.
Define Alert Criteria	Select whether alerts need to be generated based on incoming traffic, outgoing traffic, or both. The default setting is for both(combined). Then select the application / port for which the alert has to be generated. This criteria can be very general - Any application traffic can be profiled - or it can be highly specific - Generate the alert only when a specific application, protocol, and/or port is used. To identify the overall link utilization the "No Criteria" option has to be chosen
Define Threshold and Action	Enter the threshold conditions (threshold utilization, no. of times it can exceed and the time duration) exceeding which the alert will be generated. You can also specify an action to be taken during the alert creation. - Email - to send a notification, along with a <b>PDF attachment</b> , to one or more


Field	Description
	people. - SNMP Trap - to send a trap to the manager application (specify the <server name>:<port>:<community>). For details on configuring trap forwarding, refer to SNMP Trap Forwarding section under Appendix To add more threshold values, click 'Add Row' and add values

### Customizing from address:

You can customize the "From Address" from the mail server settings in Settings page.

After setting the required thresholds, click '**Save**'

The new alert profile is created and activated. The system watches the utilization and raises alarms when the specified conditions are met.

	<p>Only one alert is generated for a specified time duration. For example, say for a particular interface, the threshold is set as 60% and number of times is set as 3 times and the time duration is set as 30 minutes. Now lets assume that the utilization in that interface goes above 60% and stays above it. Then in 3 minutes, the above conditions will be met and an alert will be generated. The next alert will NOT be generated after 6 minutes, but only in the 33rd minute, if the condition persists. Thus for the specified 30 minutes time duration, only one alarm is generated. This is designed to avoid a lot of repetitive mail traffic.</p>
---	--

### Modifying or Deleting Alert Profiles

Select an alert profile, and click on **Modify** to modify its settings. You can change all of the alert profile's settings except the profile name. However, it is possible to modify the "Link Down" alert profile's name. There is also an option to clear details of all alerts created for this profile from this page itself. Once you are done, click **Save** to save your changes.

Select an alert profile, and click on **Delete** to delete the profile. Once an alert profile is deleted, all alerts associated with that profile are automatically cleared. However it is not possible to delete the "Link Down" alert profile

## Schedule Reports



It is a good idea to schedule reports to be run at non-peak traffic hours since generation of reports is a resource hungry process especially for large interface numbers.



An easy scheduling option is available in NetFlow Analyzer for any particular interface while drilling down. Click on the "Actions" tab on the top right and from the dropdown options click on "Add Schedule". You can give a schedule name, description and other scheduling options as per your requirement.

A Scheduler is configured to set the parameters for automating the generation of reports. The parameters to be set for creating a Scheduler are:

- **Source** - The Interfaces or IP Groups which are the source of traffic.
  - **Interfaces** - The list of interfaces who's bandwidth utilization must be watched. One report will be generated for each interface selected
  - **IP Groups** - The IP groups who's bandwidth utilization must be watched. One report will be generated for each IP Group created
- **Report Type** - The type of report to be generated - Please select as per your requirement from the dropdown consisting the following:
  - Consolidated report
  - Traffic report
  - Application report
  - Source report
  - Source network report
  - Destination report
  - Destination network report
  - QoS report
  - Conversation report
  - Conversation network report
  - Custom report
  - NBAR report
  - CBQoS report
- **Report Generation Schedule** - How and when the report is to be generated (e.g.) daily, weekly, monthly, or only once
  - **Generate report on** - This value determines the time when report is to be generated
  - **Generate report for** - This value determines the start and the end time for the report
- **Email Address** - This is the address to which the generated reports will be sent

Netflow Analyzer calculates the bandwidth utilization on the specified interfaces / IP Groups every minute. Based on the schedule opted for, reports are generated at various time intervals. The **Schedule Reports** feature lets you Create new Schedules and Delete existing ones. The Scheduler List page lists all existing schedules, along with the Schedule details, Status, Report types, and the Last Report Generated time.

The various columns displayed in the Scheduler List page are described in the table below:

Column	Description
Name	The name of the Schedule when it was created. Click on the Schedule's name to see more information about the schedule's configuration
Schedule Details	Information on when the schedule will run
Status	By default all schedules are Enabled, which means they are active. Click the  <b>Enabled</b> icon to disable a schedule. When this is done, reports will no longer be generated for that configuration. Click the  <b>Disabled</b> icon to enable the schedule again
Report Type	Whether it is a consolidated report or user-defined Custom report
Last Report Time	This column lists the last time when this schedule was run and a report created
Generated Reports	By clicking on View Reports it is possible to view all the previous reports that have been generated. The number of reports that are stored is based on the user definition in the Schedule Setting page. (By enabling the item "Enable older reports to be accessed from UI" it is possible to retrieve even older reports.) For Daily Schedule up to 90 reports can be stored. For Weekly Schedule up to 104 reports can be stored. For Monthly Schedule up to 60 reports can be stored.

## Operations on Schedule Reports

You can create new schedules or delete existing ones from the Schedule List page.

The "**Schedule settings**" tab on the right lets you define settings needed for the schedule reports. The settings are:

- Host name options - Select the option as you want to view in the reports. IP Address or DNS names
- Graph options - Either of the two options can be selected : utilization graph as percentage OR speed graph in bps
- Mail attachment options - If you like the attachments as ZIP or PDF. In case you select PDF, you can also select the number of PDF's you want attached with the mail
- QoS options - You can select between DSCP and ToS

You can also enable the option to access older reports from the UI.

## Configuring a new Schedule

The steps to configure a Schedule are:

1. Login to the NetFlow Analyzer client and click "**Schedule Reports**" under "**Admin Operations**" in the left panel
2. Click "**Add**" to add a new Schedule Profile
3. Fill in the following details

Field	Description
Scheduler Name	Enter a unique name to identify this scheduler.
Description	Enter descriptive information for this scheduler profile to help other operators understand why it was created.
Select Source	By default all managed interfaces sending NetFlow exports are selected. If you want this schedule configuration to apply to certain interfaces only, click the <b>Modify Selection</b> link. In the pop-up window, select the required devices and interfaces and click <b>Update</b> to save your changes.

Field	Description
	By default all IP Groups are selected. If you want this schedule configuration to apply to certain IP Groups only, click the <b>Modify Selection</b> link. In the pop-up window, select the required devices and IP Groups and click <b>Update</b> to save your changes.
Report Type	Select whether the reports that need to be generated from the srop-down. It consists of consolidated, traffic, source, NBAR, custom, QoS reports or many more available options.
Schedule Report Generation	Select the report generation frequency as one from : Daily, Weekly, Monthly and Only Once. Depending on this the report will be generated at the appropriate time intervals.
Email Address to Send Reports	Enter the email address to which the generated reports have to be emailed. You can enter multiple email addresses separated by a comma.


After setting the required parameters, click 'Save'

### Custom Report :

Opting for custom report lets you set criteria on the basis of which the report will be generated. By clicking on the "Add Criteria" button one can set a matching condition on "Source Address, Source Network, Source Nodes, Destination Address, Destination Network, Destination Nodes and Application". To add more criteria click on "Add Criteria" again. Having created all the criterions you can decide whether to make the generated report to match all of the criterions created or any of them.

### Scheduling Report Generation

The report generation schedule can be chosen from one of the following:

- Daily** - When you opt for "Daily" you have the option to set the time at which the report should be generated. Also, the report could be generated for the previous day, the last 24 hours or any of the options available in the dropdown. When the "Previous Day" option is opted the report is generated for the time period from 00:00 hours to 23:59 hours of the previous day. You have the option to narrow down this time period by using the time filter - . For instance if the maximum flow happens during your working hours from 08:00 hours to 18:00 hours you can set it in the window that pops up.

When you opt for the last 24 hours then the report is generated for the flow in the intervening 24 hours (from the time at which the report is to be generated today). The 30 most recent reports for this schedule can be accessible from the Schedule List page

### Exclude weekends:

When you choose the Exclude Weekend option with "Previous day", reports will be generated on Tuesday, Wednesday, Thursday, Friday and Saturday. These will be reports pertaining to Monday, Tuesday, Wednesday, Thursday and Friday respectively.

When you choose the Exclude Weekend option with "Last 24 hours", reports will be generated on Monday, Tuesday, Wednesday, Thursday and Friday.

- Weekly** - When you opt for the "Weekly" option, you have the option to specify the day and time at which the report needs to be generated. The report could be generated for the previous day, the last 24 hours or any of the options available in the dropdown. By additionally opting for the "Exclude Weekend" the report can be made to include only data corresponding to monday through friday.



The previous week option would generate the report for the time period Sunday 00:00 hours till Saturday 23:59 hours. When "Exclude Weekends" is enabled the report will be generated for the time period Monday 00:00 hours till Friday 23:59 hours.

The "Last 7 Days" option would generate the report for the last 7 days from the time at which the report is to be generated. Again, the exclude weekend option would generate for the last 7 days with the data for the weekend (saturday,sunday) excluded. For instance if the report is to be generated at Monday 10:00 am, with the rules set as "last 7 days" and "Exclude weekend" enabled, then the report will be generated for the time period last week's Monday 10:00 hours to Friday 23:59 hours and from this week Monday's 00:00 hours till 10:00 hours. The 52 most recent reports for this schedule can be accessible from the Schedule List page

- **Monthly** - By opting for the "Monthly" option you can set the date of the month along with the time at which the report needs to be generated every month . The report could be generated for the previous day, the last 24 hours or any of the options available in the dropdown. By selecting "Exclude Weekends" the report can be made to include only data corresponding to monday through friday.

When "Previous Month" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated for the whole of last month ( first to the last day of the month). When "Exclude weekend" option is enabled then the generated report will exclude all the intervening weekends (saturday & sunday).

When "Last 30 Days" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated from last month's 5-th 10:00 hours till this month 5-th's 10:00 hours. When "Exclude Weekend" option is enabled then the generated report will exclude all the intervening weekends(saturday & sunday). The 12 most recent reports for this schedule can be accessible from the Schedule List page.

- **Only Once** - If you wish to generate report only once at a specified time you can do that by opting for "Only Once". The date and time at which the report should be run can be specified. The date & time can be altered by using the icon - . The report could be generated for the Previous Day, Last 24 Hours, Previous Week, Last 7 Days, Previous Month, Last 30 Days or other options from the drop down. When "Previous Day" option is enabled then the  button permits the setting of working hours. The latest report for this schedule can be accessible from the Schedule List page.

### Customizing from address:

You can customize the "From Address" from the mail server settings in settings.

### A note on emailed reports:

A report is generated for each interface / IP Group - 50 such reports are zipped in a single email and mailed. In case of more than 50 interface/ IP Groups selected the report will be sent in multiple emails. The last generated reports for all schedules will be under the folder NetFlow -> Reports.

### Deleting Schedules

Select a schedule from the Schedule List and click on **Delete** to delete the schedule. Once a schedule is deleted no longer reports are generated at the stipulated intervals. Deleting a schedule also deletes the corresponding folder.

## Schedule Settings

In addition, there is the **Schedule Settings** link in the Schedule List Page. This link lets you set parameters that could be applied across all the generated reports. The parameters include:

- **Host Name display in reports** - This determines how the host name is displayed in reports. It could be chosen as one of
  - IpAddress ( or )
  - DNS Name
- **Graph Options (Report Type to be shown in reports)** - This determines how the data is to be shown in the generated reports. This could be one of
  - Utilization (in %) ( or )
  - Speed (in bps)
- **Report Mail-Attachment option** - The format in which the attachments are to be mailed. It could be one of
  - Zipped file ( or )
  - PDF - The number of PDF files to be sent in a mail is to be specified. The number may range from 5 to 50 in increments of five
- **Enable older reports to be accessed from UI**
  - Daily Schedules - the number of daily reports to be stored ( it can take values of 7 / 30 / 60 / 90 )
  - Weekly Schedules - the number of weekly reports to be stored ( it can take values of 4 / 26 / 52 / 104 )
  - Monthly Schedules - the number of monthly reports to be stored ( it can take values of 12 / 36 / 60 )

Once the schedule settings have been configured, click on the "Save" button to apply this settings from hereon. Also click on "Close" button to close the window and proceed to the Schedule List page.

## Device Group Management

---

NetFlow Analyzer lets you create device groups, which consist of a set of routers. A device group can contain any number of routers, and a router can belong to any number of device groups.

The **Device Group Management** option lets you create, manage, and delete device groups. Initially, when no device groups have been created, you will see a message that lets you start creating device groups.



The options visible under the **Admin Operations** menu depend on the user level you have logged in as. Look up User Management to know more about user levels and the respective administrative operations allowed.

### Creating a Device Group

Follow the steps below to create a new device group:

1. Click the **Add** button to create a new device group
2. Enter a unique name to identify the device group. The same name is displayed in the Device Group menu on the left, and will be listed under Available device groups when managing a user.
3. Use the **Device Group Description** box to enter useful information about the device group
4. Select the routers needed for this device group from the list of available routers displayed

Once all values have been entered, click the **Update** button to create this device group and begin generating traffic reports for the same.

### Managing a Device Group

Select an existing device group and click the **Modify** button to modify its properties. You can change all properties of the device group except its name. Once you have made changes to the properties of this device group, click the **Update** button to save your changes.

Select an existing device group and click the **Copy** button to copy its settings. This is useful when you need to create a new device group that includes the same routers as that of this device group. This saves you the trouble of adding the routers all over again. Then follow the same steps as those in creating a new device group.

Select a device group and click the **Delete** button to delete the device group. When a device group is deleted, it is removed from the Device Group List and the Device Group menu. All users assigned to this device group will not see this device group on their Dashboard.

### Interface Group

Interface Group allows you to combine interfaces in order to monitor traffic. This can be useful for grouping multiple sub-interfaces into a single logical entity. Follow the steps below to create a new interface group:

1. Click the **Interface Group** tab next to the Device Group tab
2. Enter a name to identify the interface group in the **Interface Group Name** box .
3. Use the **Interface group speed** box to enter the speed limit for the interface group
4. Select the routers needed and the interfaces under them for this interface group. By selecting a router ,by default, all interfaces are selected. You can selectively unselect the unwanted interfaces from the list.
5. Click on **Add** to save the changes.

The Interface group that is created is listed in the Dashboard view in the "Interface View" tab. The Interface group name, the In-Traffic & Out-Traffic for the last 1 hour can be seen in it. By clicking on the interface group name it is possible to further drill down to view further details. To delete a particular interface group select the interface group and click on delete

### **Modifying an interface group:**

You can modify any interface group, later, by selecting the particular interface group to be modified and clicking on the "**Modify**" tab.

## Billing

Billing is the latest feature introduced in NetFlow Analyzer. This feature helps keep a tab on resource usage and takes the bandwidth monitoring one step ahead - Accounting. It makes easy to understand the reports in terms of cost incurred. Internally, organizations can use this feature for department-wise billing. Also Internet Service Providers can use this to automatically generate reports for their customers.

### Operations on Billing

Billing can be accessed through "**Billing**" in "**Admin Operations**"

### Creating a Bill Plan

A bill plan can be created on basis of either one of the following:

1. Speed
2. Volume

#### Speed based billing:

The "**Bill Plan List**" tab lets you create a new bill plan. To create a bill plan, click on the "**Add Plan**" tab. The Fields and their description are given below.

#### Enter Billing Details

Field	Description
<b>Bill Plan</b>	Enter the name you wish to assign for this bill plan
<b>Bill Plan Description*</b>	Describe the plan for detailed understanding and for future reference
<b>Billing Type</b>	Select " <b>speed</b> "
<b>Base Speed</b>	Enter the base speed of the connection in bps (bits per second)
<b>Base Cost</b>	Select the currency from the drop-down box and enter the cost
<b>Additional Speed*</b>	Enter the additional speed of the connection in bps
<b>Additional Cost*</b>	Enter the cost for additional usage
<b>95th Percentile Calculation</b>	Select one of the two options from the drop-down box. Selecting " <b>In &amp; Out merge</b> " will merge the In and Out values and calculate the 95 percentile value. Selecting " <b>In &amp; Out separate</b> " will calculate 95th percentile value of IN and 95th percentile value of OUT separately and the higher of the two is considered. This is calculated using 5 minutes average data points. For better understanding, see the example.
<b>Billing Period</b>	Lets you select the option as quarterly or monthly. In case you select the billing plan as <b>quarterly</b> , the bill will be generated quarterly on the date you specify in the " <b>Bill generation date</b> " option. In case you select the billing plan as <b>monthly</b> , the bill will be generated on a monthly basis on the date you specify in the " <b>Bill generation date</b> " option.
<b>Bill Generation Date</b>	Enter the date on which you want the bill to be generated either on monthly basis or quarterly basis.

\* - optional fields. Other fields are mandatory.

**Associated To**

This has the list of Routers/interfaces and IP groups. You can select the interfaces and/or the IP groups that is associated with this plan.



Once an Interface/IP Group is added to one bill plan, the specific interface/IP Groups does not get displayed while creating other bill plans

**Email ID To Send Reports**

Enter the mail ID/IDs to which the generated Bill report needs to be sent. Multiple mail IDs should be separated by comma ","

Example for the 95th Percentile calculation:

**IN & OUT MERGE:**

**inbound** = [0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157]

**outbound** = [1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002]

**Inbound and Outbound merge**

= [0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157 1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002]

**Sorted\_In & Out**= [3.988 1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.971 0.940 0.896 0.874 0.689 0.653 0.523 0.438 0.370 0.347 0.231 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032]

Sorted In and Out contains set contains 40 samples--5% of 40 is 2, so discarding the top 5% means we must discard the top two samples from the data set. We are now left with:

**Sorted\_In & Out**= [1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.971 0.940 0.896 0.874 0.689 0.653 0.523 0.438 0.370 0.347 0.231 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032]

The highest sample from remaining data set is the 95th percentile value for the originating set. So we obtain the following value:

**95th\_in & out = 1.427 Mbps**

**IN & OUT SEPERATE:**

**inbound** = [0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157]

**outbound** = [1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002]

After sorting, we obtain:

**sorted\_in** = [0.971 0.653 0.370 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032]

**sorted\_out** = [3.988 1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.940 0.896 0.874 0.689 0.523 0.438 0.347 0.231]

Each sample set contains 20 samples--5% of 20 is 1, so discarding the top 5% means we must discard the top sample from each data set. We are now left with:

```
remaining_in = [0.653 0.370 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157
0.139 0.131 0.126 0.116 0.084 0.047 0.032]
remaining_out = [1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.940
0.896 0.874 0.689 0.523 0.438 0.347 0.231]
```

The highest sample from each remaining data set is the 95th percentile value for the originating set. So, for each set, above, we obtain the following values:

```
95th_in = 0.653 Mbps
95th_out = 1.435 Mbps
```

The higher of the two computed 95th percentile values becomes the final 95th percentile value used for billing:

**95th percentile = 1.435 Mbps**

Volume based billing:

The "Bill Plan List" tab lets you create a new bill plan. To create a bill plan, click on the "Add Plan" tab. The Fields and their description are given below.

**Enter Billing Details**

Field	Description
<b>Bill Plan</b>	Enter the name you wish to assign for this bill plan
<b>Bill Plan Description*</b>	Describe the plan for detailed understanding and for future reference
<b>Bill Type</b>	Select "Volume"
<b>Base Volume</b>	Enter the base volume in bytes
<b>Base Cost</b>	Select the currency from the drop-down box and enter the cost
<b>Additional Volume*</b>	Enter the additional volume in bytes
<b>Additional Cost*</b>	Enter the cost for additional usage
<b>Data transfer calculation</b>	Select one of the three options from the drop-down box. Selecting "Download" will take only downloaded data for billing. Selecting "Upload" will take only uploaded data for billing. Selecting "Download & Upload" will take both uploaded and downloaded data for billing.
<b>Alert</b>	Checking this box will activate threshold based alerting. This will send alerts, if the user specified threshold value has been exceeded.
<b>Billing Period</b>	Lets you select the option as quarterly or monthly. Incase you select the billing plan as <b>quarterly</b> , the bill will be generated quartely on the dateyou specify in the " <b>Bill generation date</b> " option. Incase you select the billing plan as <b>monthly</b> , the bill will be generated on a monthly basis on the date you specify in the " <b>Bill generation date</b> " option.
<b>Bill Generation Date</b>	Enter the date on which you want the bill to be generated either on monthly basis or quartely basis.

\* - optional fields. Other fields are mandatory.

**Associated To**

This has the list of Routers/interfaces and IP groups. You can select the interfaces and/or the IP groups that is associated with this plan.



Once an Interface/IP Group is added to one bill plan, the specific interface/IP Groups does not get displayed while creating other bill plans

### Email ID To Send Reports

Enter the mail ID/IDs to which the generated Bill report needs to be sent. Multiple mail IDs should be separated by comma ","

### On-Demand Billing

Bills can be generated on demand. By clicking on "OnDemand" for a particular bill plan in the bill plan list, a bill can be generated for the time period from the beginning of the billing cycle to the current date.

### Editing Bill Plan

Bill plans can be edited by clicking Bill plans list and editing any particular bill as the need may be.

### Adding an interface/IP group

An interface/IP group can be added during any point of the billing cycle. The bill will be generated for this interface/IP group during the mentioned billing date for the billing plan.

### Removing an interface/IP group

When an Interface/IP group is removed from a bill plan, the bill for that interface is generated at the same instant.

### Other billing parameters

Editing **base speed / volume, base cost, additional speed / volume, additional cost, billing calculation (95th Percentile / Data transfer)** will take effect only from the next billing cycle. Editing email ID and threshold alerting will take effect at the same time.



"**Billing period**" and "**Bill generation date**" CANNOT be changed. When the interfaces/ IP groups are unmanaged/ deleted, bill is generated for the interface or IP groups at that instant. If you modify the cost in the bill plan, It will be effected from the next billing cycle and NOT at that instant.

### Deleting Bill Plan

Deleting a bill plan will lead to deletions of all the reports generated by the particular bill plan.

### Reports

Generated Reports can be viewed by clicking the "**Report**" tab on top.

### Available plans

You can view all the plans or any one plan by selecting the suitable option from the drop-down box. By default the "report" page shows only the recent report of all the bill plans. If you want to view all the generated reports for a particular bill plan, select the bill plan from the drop-down box, next to "available plans". The reports are arranged with the most recent report on top.

### **Show details**

By clicking on "show details" a pop up window opens, wherein you can view a speed-time graph. This shows all the bills generated for the particular interface. The report in can be generated in PDF format by clicking on "**PDF**" and you can view the data at 5 minutes interval by clicking on the "**Data points**"

## NBAR

### NBAR Reporting

---

#### What is NBAR?

NBAR (Network Based Application Recognition) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications like Web-based and client/server applications. It can analyze & classify application traffic in real time. NBAR is supported in most Cisco switches and routers and this information is available via SNMP. Click here to view the list of protocols that are recognized by NBAR.

#### Why do I need NBAR?

NBAR, by adding intelligent network classification to your infrastructure, helps in ensuring that the network bandwidth is used efficiently by working with QoS(Quality Of Service ) feature. With NBAR, network-traffic classification becomes possible and by this we can know how much of say , HTTP traffic is going on. By knowing this, QoS standards can be set. Unlike NetFlow, which relies on port & protocol for application categorization, NBAR performs a deep-packet inspection and allows you to recognize applications that use dynamic ports. Also, the NBAR approach is useful in dealing with malicious software using known ports to fake being "priority traffic", as well as non-standard applications using non-determinaly ports.

#### How do I enable NBAR?

You will first have to check whether your router supports NBAR. Please visit here to know about the Platforms & IOS that support NBAR. NBAR can be enabled only on those interfaces which are identified by NetFlow Analyzer.

If your router supports NBAR, then you will have to enable NBAR on each of the interface that you want to collect NBAR statistics.

NBAR can be enabled in two ways:

- Enabling on the device
- Enabling from the NetFlow Analyzer user interface

#### Enabling on the device

The following is a set of commands issued on a router to enable NBAR on the FastEthernet 0/1 interface.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#ip cef
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip nbar protocol-discovery
router-2621(config-if)#exit
router-2621(config)#exit
router-2621(config)#show ip nbar protocol-discovery
```



Please note that the part in red has to be repeated for each interface individually.

## Enabling from NetFlow Analyzer User Interface

Alternately, you may check the router's NBAR supported status and also enable NBAR on the interfaces from the NetFlow Analyzer's NBAR Configuration page. The steps to enable from User Interface are:

1. Under **NBAR enabled interfaces** : You will first have to enable NBAR on an interface before you can start collecting NBAR data. This step allows you to enable NBAR on the interface. Enabling NBAR on the interface is done through SNMP and requires SNMP write community.
  1. Use the "Click Here" link to enable NBAR on Interfaces.
  2. Set SNMP Read Community, SNMP Write Community & the Port, in case you want to alter the default parameters. The values given during installation are prepopulated in the screen.
  3. Click on "Check Status" to see if the interfaces on the router have NBAR enabled on them. Click on "Check all Status" at the top of the window to know the NBAR support status of all the interfaces (under various routers). At the end of the status check a message is displayed at the bottom of the window( of each router pane). If NBAR has been enabled on the interfaces then the message " Success : NBAR status of the interfaces updated" is displayed. If the Check Status operation didnt succeed, due to SNMP error or Request Time-Out, then the message "SNMP Error : NBAR status of the interfaces not updated" is displayed. Also NBAR support is displayed as 'Yes' or 'Unknown' under the router name as the case may be.
    - In the right pane the status of each interface is shown under "NBAR Status". If NBAR is enabled on all interfaces then the status is shown as "Enabled" against each of the interfaces in that router.
  4. Select the interfaces you want NBAR to be enabled on(which are currently not enabled).
  5. Click on "Enable NBAR".
  6. If NBAR is enabled on the interface then the status will be displayed as "Enabled" against each of the selected interfaces. If NBAR cannot be enabled on the interface then the status will be displayed in red (Unknown or Disabled).

## How do I disable NBAR?

Disabling NBAR can be done in two ways.

- Disabling on the device
- Disabling from the NetFlow Analyzer user interface

## Disabling on the device

The following is a set of commands issued on a router to disable NBAR on the FastEthernet 0/1 interface.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#no ip nbar protocol-discovery
router-2621(config-if)#exit
router-2621(config)#exit
```



Please note that the part in red has to be repeated for each interface individually.

## Disabling from NetFlow Analyzer User Interface

The steps to disable from User Interface are:

1. Under **NBAR enabled interfaces**: This step allows you to disable NBAR on the interface. Disabling NBAR on the device is done through SNMP and requires you to provide the SNMP write community.
  1. Click on "Modify Interfaces".
  2. Set SNMP Read Community, SNMP Write Community & the Port, in case it is not already set.
  3. Select the interfaces on which you want to disable NBAR and click on "**Disable NBAR**".
  4. If NBAR is disabled on the interface then the status will be displayed as "Disabled" against each of the selected interfaces. If NBAR cannot be disabled on the interface then the status will be displayed in red (Unknown or Enabled).

## Polling

What is Polling - The process of sending the SNMP request periodically to the device to retrieve information ( Traffic usage/ Interface Statistics in this case ) is termed polling. A low polling interval (of say 5 minutes) gives you granular reports but may place an increased load on your server if you poll large amount of interfaces. Time out value needs to be set to a higher value in case your routers are at remote locations.

After NBAR has been enabled on select interfaces the polling can be started on those interfaces.

## Start Polling

Polling can be done on those interfaces on which NBAR has been enabled earlier. Please do the following to start polling on an interface:

1. Under "**Polling for NBAR data**" :
  1. Use the link "click here " to invoke the screen which lists the NBAR enabled interfaces.
  2. Select the interfaces on which you want to do polling.
  3. Set the Polling Parameters - the Polling Interval & the Time Out. The Polling interval decides the frequency at which the NetFlow Analyzer server will poll the device. Time out is the amount of time for which NetFlow Analyzer server waits for the SNMP response from the device.
  4. Click "**Update**" to update the Polling Parameters.

## Stop Polling

Polling can be stopped on those interfaces by following these steps.

1. Under "**Polling for NBAR data**" :
  1. Use the "Modify Poll Parameters" to invoke the screen, which lists the already polled interfaces with the check box selected and the "Polling Status" set as "Polling".
  2. Unselect the interfaces on which you want to stop polling.
  3. Click "**Update**" to stop polling.




The default NBAR data storage period is 2 months. You can change the storage period from Raw Data Settings under Settings page.

## NBAR Report

---

The **NBAR Report** tab lists the various applications in your network and their percentage of the total traffic for the selected time period. The default view shows the **NBAR Application - In Report**. This report shows the distribution of traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.

Click "**Supported Applications**" link to see the list of supported applications, in a new window.

### Viewing Top Applications

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.

The pie chart below shows what percentage of bandwidth is being used by each Application. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can the export as a PDF, CSV file or email the report by going to the "Actions" button on top and selecting as per your requirement

## NBAR Supported Applications

NBAR supports a wide range of network protocols. The following list shows some of the supported protocols:

### 1. Peer-to-Peer Protocols

Peer-to-Peer Protocol	Type	Description
BitTorrent	TCP	File-sharing application
Gnutella	TCP	File-sharing application
Kazaa2	TCP	File-sharing application
eDonkey	TCP	File-sharing application
Fasttrack	TCP	File-sharing application
Napster	TCP	File-sharing application

### 2. VoIP Protocols

VoIP Protocol	Type	Description
SCCP	TCP	Skinny Call Control Protocol
SIP	TCP and UDP	Session Initiation Protocol
MGCP	TCP and UDP	Media Gateway Control Protocol
H.323	TCP and UDP	An ITU-T standard for digital videoconferencing over TCP/IP networks
SKYPE	TCP and UDP	Application allowing telephone conversation over the Internet

### 3. TCP & UDP stateful protocols

TCP or UDP Stateful Protocol	Type	Description
FTP	TCP	File Transfer Protocol
Exchange	TCP	MS-RPC for Exchange
HTTP	TCP	HTTP with URL, host, or MIME classification
Citrix	TCP	Citrix published application
Netshow	TCP/UDP	Microsoft Netshow
RealAudio	TCP/UDP	RealAudio Streaming Protocol
r-commands	TCP	rsh, rlogin, rexec
StreamWorks	UDP	Xing Technology Stream Works audio/video
SQL*NET	TCP/UDP	SQL*NET for Oracle
SunRPC	TCP/UDP	Sun Remote Procedure Call
TFTP	UDP	Trivial File Transfer Protocol
VDOLive	TCP/UDP	VDOLive streaming video

4. Non- TCP & Non-UDP protocols

Non-UDP or Non-TCP Protocol	Type	Well-Known Port Number	Description
EGP	IP	8	Exterior Gateway Protocol
GRE	IP	47	Generic Routing Encapsulation
ICMP	IP	1	Internet Control Message Protocol
IPINIP	IP	4	IP in IP
IPsec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol

5. TCP & UDP static port protocols

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
BGP	TCP/UDP	179	Border Gateway Protocol
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing
CU-SeeMe	UDP	24032	Desktop videoconferencing
DHCP/Bootp	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	53	Domain Name System
Finger	TCP	79	Finger User Information Protocol
Gopher	TCP/UDP	70	Internet Gopher Protocol
HTTP	TCP	80	Hypertext Transfer Protocol
HTTPS	TCP	443	Secured HTTP
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol
IRC	TCP/UDP	194	Internet Relay Chat
Kerberos	TCP/UDP	88, 749	The Kerberos Network Authentication Service
L2TP	UDP	1701	L2F/L2TP Tunnel
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol
MS-SQLServer	TCP	1433	Microsoft SQL Server top videoconferencing
NetBIOS	TCP	137, 139	NetBIOS over IP (Microsoft Windows)
NetBIOS	UDP	137, 138	NetBIOS over IP (Microsoft Windows)
NFS	TCP/UDP	2049	Network File System
NNTP	TCP/UDP	119	Network News Transfer Protocol
Notes	TCP/UDP	1352	Lotus Notes
NTP	TCP/UDP	123	Network Time Protocol
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere
POP3	TCP/UDP	110	Post Office Protocol
PPTP	TCP	1723	Point to Point Tunneling Protocol
RIP	UDP	520	Routing Information Protocol

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
RSVP	UDP	1698,1699	Resource Reservation Protocol
SFTP	TCP	990	Secure FTP
SHTTP	TCP	443	Secure HTTP
SIMAP	TCP/ UDP	585, 993	Secure IMAP
SIRC	TCP/ UDP	994	Secure IRC
SLDAP	TCP/ UDP	636	Secure LDAP
SNNTTP	TCP/ UDP	563	Secure NNTP
SMTP	TCP	25	Simple Mail Transfer Protocol
SNMP	TCP/ UDP	161, 162	Simple Network Management Protocol
SOCKS	TCP	1080	Firewall security protocol
SPOP3	TCP/ UDP	995	Secure POP3
SSH	TCP	22	Secured Shell
STELNET	TCP	992	Secure TELNET
Syslog	UDP	514	System Logging Utility
Telnet	TCP	23	Telnet Protocol
X Windows	TCP	6000-6003	X11, X Windows

## NBAR supported platforms & IOS Versions

---

Platforms & Cisco IOS Versions that currently support **CISCO-NBAR-PROTOCOL-DISCOVERY-MIB** are

- Cisco 1700 Series Router since Release 12.2(2)T
- Cisco 2600, 3600, 7100, 7200 Series Routers since Release 12.1(5)T
- Cisco 3700 and 7500 Series Routers since Release 12.2(8)T

The following Platforms also support NBAR:

- Cisco 800 Series Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 2600XM Series Router
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7300 Series Routers
- Cisco 7400 Series Routers
- Catalyst 6500 Family Switch with a FlexWAN card.

To know the supported IOS versions check [here](#)

## Flexible NetFlow and NBAR integration

If a router supports flexible netflow (FNF), then the NBAR data can be collected without polling. To do so,

1. Go to the interface from NetFlow Analyzer.
2. Click on the "NBAR" tab for that interface.
3. In the NBAR tab, click on the "FNF" radio button

### Configuring Flexible NetFlow for Network Based Application Recognition

The FNF/NBAR feature is easily enabled by configuring an additional "**application name**" field in the flow record configuration sub-mode.

This may be configured as a key field under the "**match**" keyword, or as a non-key field under the "**collect**" keyword.

```
router (config-flow-record) #match application name
```

The flow record is then configured in flow monitors, and the flow monitors configured on interfaces as usual for Flexible NetFlow.

Example:

The following example uses Network Based Application Recognition (NBAR) to create different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key field.

This sample starts in global configuration mode:

```
!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

### Flexible Netflow Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Flexible NetFlow	"Cisco IOS Flexible NetFlow Overview"
Flexible NetFlow Feature Roadmap	"Cisco IOS Flexible NetFlow Features Roadmap"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS"

Related Topic	Document Title
	Flexible NetFlow"
Configuring flow exporters to export Flexible NetFlow data.	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	"Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic"
Configuring Flexible NetFlow using predefined records	"Configuring Cisco IOS Flexible NetFlow with Predefined Records"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"
Configuring IPv4 multicast statistics support for Flexible NetFlow	"Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow"
Configuration commands for Flexible NetFlow	Cisco IOS Flexible NetFlow Command Reference

## CBQoS

---

### What is CBQoS ?

CBQoS (Class Based Quality of Service) is a Cisco feature set that is part of the IOS 12.4(4)T and above. This information is retrieved using SNMP and provides information about the QoS policies applied and class based traffic patterns within an enterprise's network.

### Why do I need CBQoS ?

Typically, networks operate on the basis of best-effort delivery, in which all traffic has equal priority and an equal chance of being delivered. When congestion results, all traffic has an equal chance of being dropped. QoS selects network traffic, prioritizes it according to its relative importance, and uses congestion avoidance to provide priority-indexed treatment; CBQoS can also limit the bandwidth used by network traffic. CBQoS can make network performance more predictable and bandwidth utilization more effective. Network administrators implement CBQoS policies to ensure that their business-critical applications receive the highest priority on the network. CBQoS provides you in depth visibility into the policies applied on your links and the traffic patterns in your various class of traffic. The pre-policy, post-policy and drops in different traffic class along with the queuing status enables you to validate the efficiency of your QoS settings.

- Creating a traffic class
- Creating a traffic policy
- Attaching a Traffic Policy to an Interface
- Verifying the Traffic Class and Traffic Policy Information

### How do I start CBQoS data collection ?

#### Configuring Policies on the router

Initially CBQoS has to be enabled on the router manually. Further, policies have to be defined on the router. Usually, Traffic Policies are dependent on the type of the enterprise and its business needs.( heavy voice traffic, heavy document transfer, heavy streaming video traffic etc ). The policy (classification ) can be done on the basis of Class Maps and Policy Maps.

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criterion used to match against a specific traffic flow to further classify it; the criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you can specify the QoS actions via a policy map. A policy map specifies the QoS actions for the traffic classes. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to an interface.

After a packet is classified and has an internal DSCP value assigned to it, the policing and marking process has to be done. Policing involves creating a policy that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or marking down the packet with a new DSCP value that is obtained from the configurable policed-DSCP map.

## Fetching Policy details from the router

Under the QoS Configuration tab the interfaces that have policies applied on them are displayed along with the router names and specific IN and OUT Policies. To facilitate the NetFlow Analyzer application to recognize the policies applied at each router level, click on the **Check Status** icon. This invokes a new window with the List of all routers, along with their Read Community & Port details. By clicking on "Check Status" or "Check All Status" it is possible to fetch the policy details from the router about each individual interface.

Once the policy details have been fetched from the routers the following message is displayed: "Policy Details Updated". If any policy is not found the the "Not Available" message is displayed.

## Polling for CBQoS data

After setting the policies on the router and fetching the policy details polling can be started. Click on the "Modify Interfaces" button to select/unselect the interfaces on which polling has to be done. The Polling Parameters namely Polling Interval and Time Out can also be modified. The Polling interval can take any value from 5, 10, 15, 25, 30, 60. Time Out can take values from 5, 10, 15. After selecting/unselecting the list of interfaces on which Polling has to be done and after the Polling Parameters have been set click on "Update" to start the polling action.

## Creating a traffic class

To create a traffic class, use the **class-map** command. The syntax of the **class-map** command is as follows:

```
class-map [match-any | match-all] class-name no class-map [match-any | match-all] class-name
```

The **match-all** and **match-any** Keywords

The **match-all** and **match-any** keywords need to be specified only if more than one match criterion is configured in the traffic class.

The **match-all** keyword is used when *all* of the match criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class.

The **match-any** keyword is used when only *one* of the match criterion in the traffic class must be met in order for a packet to be placed in the specified traffic class.

If neither the **match-all** nor **match-any** keyword is specified, the traffic class will behave in a manner consistent with **match-all** keyword.

## About The match not Command

The **match not** command, rather than identifying the specific match parameter to use as a match criterion, is used to specify a match criterion that prevents a packet from being classified as a member of the class. For instance, if the **match not qos-group 6** command is issued while you configure the traffic class, QoS group 6 becomes the only QoS group value that is not considered a successful match criterion. All other QoS group values would be successful match criteria.

## Procedure

To create a traffic class containing match criteria, use the **class-map** command to specify the traffic class name. Then use one or more **match** commands to specify the appropriate match criteria. Packets matching the criteria you specify are placed in the traffic class.



In the following steps, a number of **match** commands are listed. The specific **match** commands available vary by platform and Cisco IOS release. For the **match** commands available, see the Cisco IOS command reference for the platform and Cisco IOS release you are using.

	Command or Action	Purpose
Step 1	Router> <b>enable</b>	Enables privileged EXEC mode.
Step 2	Router # <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>class-map [match-all   match-any] class-name</b>	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class.  <b>Note :</b> The <b>match-all</b> keyword specifies that all match criteria must be met. The <b>match-any</b> keyword specifies that one of the match criterion must be met.
	Use one or more of the following <b>match</b> commands, as applicable.	
Step 4	Router(config-cmap)# <b>match access-group {access-group   name access-group-name}</b>	(Optional) Configures the match criteria for a class map on the basis of the specified access control list (ACL).  <b>Note:</b> Access lists configured with the optional <b>log</b> keyword of the <b>access-list</b> command are not supported when configuring a traffic class.
Step 5	Router(config-cmap)# <b>match any</b>	(Optional) Configures the match criteria for a class map to be successful match criteria for all packets.
Step 6	Router(config-cmap)# <b>match class-map class-name</b>	(Optional) Specifies the name of a traffic class to be used as a matching criterion (for nesting traffic class [nested class maps] within one another).
Step 7	Router(config-cmap)# <b>match cos cos-number</b>	(Optional) Matches a packet based on a Layer 2 class of service (CoS) marking.
Step 8	Router(config-cmap)# <b>match destination-address mac address</b>	(Optional) Uses the destination Media Access Control (MAC) address as a match criterion.
Step 9	Router(config-cmap)# <b>match discard-class class-number</b>	(Optional) Matches packets of a certain discard class.
Step 10	Router(config-cmap)# <b>match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value]</b>	(Optional) Identifies a specific IP differentiated service code point (DSCP) value as a match criterion. Up to eight DSCP values can be included in one match statement.
Step 11	Router(config-cmap)# <b>match field protocol protocol-field {eq [mask]   neq [mask]   gt   lt   range range   regex string} value [next next-protocol]</b>	(Optional) Configures the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs).
Step 12	Router(config-cmap)# <b>match fr-dlci dlc-number</b>	(Optional) Specifies the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map.
Step 13	Router(config-cmap)# <b>match input-interface interface-name</b>	(Optional) Configures a class map to use the specified input interface as a match criterion.
Step 14	Router(config-cmap)# <b>match ip rtp starting-port-number port-range</b>	(Optional) Configures a class map to use the Real-Time Protocol (RTP) protocol port as the match criterion.
Step 15	Router(config-cmap)# <b>match mpls experimental mpls-values</b>	(Optional) Configure a class map to use the specified value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field as a match criterion.

	Command or Action	Purpose
Step 16	Router(config-cmap)# <b>match mpls experimental topmost values</b>	(Optional) Matches the MPLS EXP value in the topmost label.
Step 17	Router(config-cmap)# <b>match not match-criteria</b>	(Optional) Specifies the single match criterion value to use as an unsuccessful match criterion.
Step 18	Router(config-cmap)# <b>match packet length</b> { <b>max</b> maximum-length-value [ <b>min</b> minimum-length-value]   <b>min</b> minimum-length-value [ <b>max</b> maximum-length-value]}	Optional) Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
Step 19	Router(config-cmap)# <b>match port-type</b> { <b>routed</b>   <b>switched</b> }	{routed   switched} (Optional) Matches traffic on the basis of the port type for a class map.
Step 20	Router(config-cmap)# <b>match [ip] precedence</b> precedence-value [precedence-value precedence-value precedence-value]	(Optional) Identifies IP precedence values as match criteria.
Step 21	Router(config-cmap)# <b>match protocol</b> protocol-name	(Optional) Configures the match criteria for a class map on the basis of the specified protocol.  Note: There is a separate <b>match protocol</b> (NBAR) command used to configure network-based application recognition (NBAR) to match traffic by a protocol type known to NBAR.
Step 22	Router(config-cmap)# <b>match protocol citrix</b> [ <b>app</b> application-name-string] [ <b>ica-tag</b> ica-tag-value]	(Optional) Configures NBAR to match Citrix traffic
Step 23	Router(config-cmap)# <b>match protocol fasttrack file-transfer</b> "regular-expression"	(Optional) Configures NBAR to match FastTrack peer-to-peer traffic.
Step 24	Router(config-cmap)# <b>match protocol gnutella file-transfer</b> "regular-expression"	(Optional) Configures NBAR to match Gnutella peer-to-peer traffic.
Step 25	Router(config-cmap)# <b>match protocol http</b> [ <b>url</b> url-string   <b>host</b> hostname-string   <b>mime</b> MIME-type   <b>c-header-field</b> c-header-field-string   <b>s-header-field</b> s-header-field-string]	(Optional) Configures NBAR to match Hypertext Transfer Protocol (HTTP) traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers.
Step 26	Router(config-cmap)# <b>match protocol rtp</b> [ <b>audio</b>   <b>video</b>   <b>payload-type</b> payload-string]	(Optional) Configures NBAR to match Real-Time Transfer Protocol (RTP) traffic.

	Command or Action	Purpose
Step 27	Router(config-cmap)# <b>match qos-group</b> qos-group-value	qos-group-value (Optional) Identifies a specific QoS group value as a match criterion.
Step 28	Router(config-cmap)# <b>match source-address</b> mac address-destination	(Optional) Uses the source MAC address as a match criterion.
Step 29	Router(config-cmap)# <b>match start</b> {I2-start   I3-start} <b>offset number</b> <b>size number</b> {eq   neq   gt   lt   range range   regex string} {value [value2]   [string]}	(Optional) Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).
Step 30	Router(config-cmap)# <b>match tag</b> {tag-name}	(Optional) Specifies tag type as a match criterion.
Step 31	Route(config-cmap)# <b>exit</b>	(Optional) Exits class-map configuration mode.

## Creating a traffic policy

To configure a traffic policy (sometimes also referred to as a policy map), use the **policy-map** command. The **policy-map** command allows you to specify the traffic policy name and also allows you to enter policy-map configuration mode (a prerequisite for enabling QoS features such as traffic policing or traffic shaping).

Associate the Traffic Policy with the Traffic Class

After using the **policy-map** command, use the **class** command to associate the traffic class (created in the "Creating a Traffic Class" section) with the traffic policy.

The syntax of the **class** command is as follows:


```
class class-name
no class class-name
```

For the *class-name* argument, use the name of the class you created when you used the **class-map** command to create the traffic class (Step 3 of the "Creating a Traffic Class" section).

After entering the **class** command, you are automatically in policy-map class configuration mode. The policy-map class configuration mode is the mode used for enabling the specific QoS features.

### Procedure

To create a traffic policy (or policy map) and enable one or more QoS features, perform the following steps.

	This procedure lists many of the commands you can use to enable one or more QoS features. For example, to enable Class-Based Weighted Fair Queuing (CBWFQ), you would use the <b>bandwidth</b> command. Not all QoS features are available on all platforms or in all Cisco IOS releases. For the features and commands available to you, see the Cisco IOS documentation for your platform and version of Cisco IOS software you are using.
---	--

	Command or Action	Purpose
Step 1	Router> <b>enable</b>	Enables privileged EXEC mode.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>policy-map</b> <i>policy-name</i>	Creates or specifies the name of the traffic policy and enters policy-map configuration mode.
Step 4	Router(config-pmap)# <b>class</b> { <i>class-name</i>   class-default}	Specifies the name of a traffic class (previously created in the "Creating a Traffic Class" section) and enters policy-map class configuration mode.
	Use one or more of the following commands to enable the specific QoS feature you want to use.	
Step 5	Router(config-pmap-c)# <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }	(Optional) Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. A minimum bandwidth guarantee can be specified in kbps or by a percentage of the overall available bandwidth.
Step 6	Router(config-pmap-c)# <b>fair-queue</b> <i>number-of-queues</i>	(Optional) Specifies the number of queues to be reserved for a traffic class.
Step 7	Router (config-pmap-c)# <b>police</b> <i>bps</i> [ <i>burst-normal</i> ][ <i>burst-max</i> ] <b>conform-action</b> action <b>exceed-action</b> action <b>violate-action</b> action	(Optional) Configures traffic policing.
Step 8	Router(config-pmap-c)# <b>priority</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percentage</i> } [ <i>burst</i> ]	(Optional) Gives priority to a class of traffic belonging to a policy map.
Step 9	Router(config-pmap-c)# <b>queue-limit</b> <i>number-of-packets</i>	(Optional) Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map.
Step 10	Router(config-pmap-c)# <b>random-detect</b> [ <b>dscp-based</b>   <b>prec-based</b> ]	(Optional) Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
Step 11	Router(config-pmap-c)# <b>set atm-clp</b>	(Optional) Sets the cell loss priority (CLP) bit when a policy map is configured.
Step 12	Router(config-pmap-c)# <b>set cos</b> { <i>cos-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet.
Step 13	Router(config-pmap-c)# <b>set discard-class</b> <i>value</i>	(Optional) Marks a packet with a discard-class value.
Step 14	Router(config-pmap-c)# <b>set [ip] dscp</b> { <i>dscp-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 15	Router(config-pmap-c)# <b>set fr-de</b>	(Optional) Changes the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.
Step 16	Router(config-pmap-c)# <b>set precedence</b> { <i>precedence-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Sets the precedence value in the packet header.
Step 17	Route(config-pmap-c)# <b>set mpls experimental</b> <i>value</i>	(Optional) Designates the value to which the MPLS bits are set if the packets match the specified policy map.

<b>Step 18</b>	Router (config-pmap-c)# <b>set qos-group</b> {group-id   from-field [table table-map-name]}	(Optional) Sets a QoS group identifier (ID) that can be used later to classify packets.
<b>Step 19</b>	Router(config-pmap-c)# <b>service-policy</b> policy-map-name	(Optional) Specifies the name of a traffic policy used as a matching criterion (for nesting traffic policies [hierarchical traffic policies] within one another).
<b>Step 20</b>	Router(config-pmap-c)# <b>shape</b> {average   peak } mean-rate [burst-size [excess-burst-size ]]	(Optional) Shapes traffic to the indicated bit rate according to the algorithm specified.
<b>Step 21</b>	Router(config-pmap-c)# <b>exit</b>	(Optional) Exits policy-map class configuration mode.

### Attaching a Traffic Policy to an Interface


To attach a traffic policy to an interface, use the **service-policy** command. The **service-policy** command also allows you to specify the direction in which the traffic policy should be applied (either on packets coming into the interface or packets leaving the interface).

The **service-policy** command syntax is as follows:


```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

#### Procedure

To attach a traffic policy to an interface, perform the following steps.

	Depending on the platform and Cisco IOS release you are using, a traffic policy can be attached to an ATM permanent virtual circuit (PVC) subinterface, a Frame Relay data-link connection identifier (DLCI), or another type of interface.
---	---

	Command or Action	Purpose
<b>Step 1</b>	Router> <b>enable</b>	Enables privileged EXEC mode.
<b>Step 2</b>	Router# <b>configure terminal</b>	Enters global configuration mode
<b>Step 3</b>	Router(config)# <b>interface serial0</b>	Configures an interface type and enters interface configuration mode.
<b>Step 4</b>	Router(config-if)# <b>service-policy output</b> [type <b>access-control</b> ] {input   output} policy-map-name	Attaches a policy map to an interface.
<b>Step 5</b>	Router (config-if)# <b>exit</b>	(Optional) Exits interface configuration mode.

	Multiple traffic policies on tunnel interfaces and physical interfaces are not supported if the interfaces are associated with each other. For instance, if a traffic policy is attached to a tunnel interface while another traffic policy is attached to a physical interface with which the tunnel interface is associated, only the traffic policy on the tunnel interface works properly.
---	--

## Verifying the Traffic Class and Traffic Policy Information

To display and verify the information about a traffic class or traffic policy, perform the following steps.

	Command or Action	Purpose
<b>Step 1</b>	Router> <b>enable</b>	Enables privileged EXEC mode.
<b>Step 2</b>	Router# <b>show class-map</b> [type {stack   access-control}] [class-map-name]	(Optional) Displays all class maps and their matching criteria.
<b>Step 3</b>	Router# <b>show policy-map</b> policy-map class class-name	(Optional) Displays the configuration for the specified class of the specified policy map.
<b>Step 4</b>	Router# <b>show policy-map</b> policy-map	(Optional) Displays the configuration of all classes for a specified policy map or all classes for all existing policy maps.
<b>Step 5</b>	Router# <b>show policy-map interface</b> [type access-control] type number [vc [vpi/] vci] [dci dci] [input   output]	(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.
<b>Step 6</b>	Router# <b>exit</b>	(Optional) Exits privileged EXEC mode.

## Using the CBQoS data

Once Polling has been started, reports can be viewed under the CBQoS tab. Reporting is available in terms of Volume of Traffic, Number of Packets, Traffic Speed and Queue. The pre-policy, post-policy and drops in different traffic class along with the queuing status enables you to validate the efficiency of your QoS settings. Individual graphs are displayed for Pre Policy, Post Policy and Dropped. Pre Policy refers to the state before the CBQoS policy was applied. Post Policy refers to the state after the CQoS policy is applied. Dropped gives information on the packets that are dropped as a result of applying the policies.

CBQoS reports can be exported as PDF, or can be mailed by going to "Actions" and clicking on the necessary action.

Based on these information suitable correction can be done to the policies to make it best suit the business goals of the organization.

## CBQoS Child Policies

Now NetFlow Analyzer lets you to create child policies under parent policies.

### Creating a traffic policy

To configure a traffic policy (sometimes also referred to as a policy map), use the **policy-map** command. The **policy-map** command allows you to specify the traffic policy name and also allows you to enter policy-map configuration mode (a prerequisite for enabling QoS features such as traffic policing or traffic shaping).

Associate the Traffic Policy with the Traffic Class

After using the **policy-map** command, use the **class** command to associate the traffic class (created in the "Creating a Traffic Class" section) with the traffic policy.

The syntax of the **class** command is as follows:


```
class class-name
no class class-name
```

For the *class-name* argument, use the name of the class you created when you used the **class-map** command to create the traffic class (Step 3 of the "Creating a Traffic Class" section).

After entering the **class** command, you are automatically in policy-map class configuration mode. The policy-map class configuration mode is the mode used for enabling the specific QoS features.

### Procedure

To create a traffic policy (or policy map) and enable one or more QoS features, perform the following steps.

	This procedure lists many of the commands you can use to enable one or more QoS features. For example, to enable Class-Based Weighted Fair Queuing (CBWFQ), you would use the <b>bandwidth</b> command. Not all QoS features are available on all platforms or in all Cisco IOS releases. For the features and commands available to you, see the Cisco IOS documentation for your platform and version of Cisco IOS software you are using.
---	--

	Command or Action	Purpose
<b>Step 1</b>	Router> <b>enable</b>	Enables privileged EXEC mode.
<b>Step 2</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	Router(config)# <b>policy-map</b> <i>policy-name</i>	Creates or specifies the name of the traffic policy and enters policy-map configuration mode.
<b>Step 4</b>	Router(config-pmap)# <b>class</b> { <i>class-name</i>   <i>class-default</i> }	Specifies the name of a traffic class (previously created in the "Creating a Traffic Class" section) and enters policy-map class configuration mode.
	Use one or more of the following commands to enable the specific QoS feature you want to use.	
<b>Step 5</b>	Router(config-pmap-c)# <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }	(Optional) Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. A minimum bandwidth guarantee can be specified in kbps or by a percentage

	Command or Action	Purpose
		of the overall available bandwidth.
Step 6	Router(config-pmap-c)# <b>fair-queue</b> <i>number-of-queues</i>	(Optional) Specifies the number of queues to be reserved for a traffic class.
Step 7	Router (config-pmap-c)# <b>police</b> <i>bps</i> [ <i>burst-normal</i> ][ <i>burst-max</i> ] <b>conform-action</b> <i>action</i> <b>exceed-action</b> <i>action</i> [ <b>violate-action</b> <i>action</i> ]	(Optional) Configures traffic policing.
Step 8	Router(config-pmap-c)# <b>priority</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percentage</i> } [ <i>burst</i> ]	(Optional) Gives priority to a class of traffic belonging to a policy map.
Step 9	Router(config-pmap-c)# <b>queue-limit</b> <i>number-of-packets</i>	(Optional) Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map.
Step 10	Router(config-pmap-c)# <b>random-detect</b> [ <b>dscp-based</b>   <b>prec-based</b> ]	(Optional) Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
Step 11	Router(config-pmap-c)# <b>set atm-clp</b>	(Optional) Sets the cell loss priority (CLP) bit when a policy map is configured.
Step 12	Router(config-pmap-c)# <b>set cos</b> { <i>cos-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet.
Step 13	Router(config-pmap-c)# <b>set discard-class</b> <i>value</i>	(Optional) Marks a packet with a discard-class value.
Step 14	Router(config-pmap-c)# <b>set [ip] dscp</b> { <i>dscp-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 15	Router(config-pmap-c)# <b>set fr-de</b>	(Optional) Changes the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.
Step 16	Router(config-pmap-c)# <b>set precedence</b> { <i>precedence-value</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Sets the precedence value in the packet header.
Step 17	Router(config-pmap-c)# <b>set mpls experimental</b> <i>value</i>	(Optional) Designates the value to which the MPLS bits are set if the packets match the specified policy map.
Step 18	Router (config-pmap-c)# <b>set qos-group</b> { <i>group-id</i>   <i>from-field</i> [ <b>table</b> <i>table-map-name</i> ]}	(Optional) Sets a QoS group identifier (ID) that can be used later to classify packets.
Step 19	Router(config-pmap-c)# <b>service-policy</b> <i>policy-map-name</i>	(Optional) Specifies the name of a traffic policy used as a matching criterion (for nesting traffic policies [hierarchical traffic policies] within one another).
Step 20	Router(config-pmap-c)# <b>shape</b> { <b>average</b>   <b>peak</b> } <i>mean-rate</i> [ <i>burst-size</i> [ <i>excess-burst-size</i> ]]	(Optional) Shapes traffic to the indicated bit rate according to the algorithm specified.
Step 21	Router(config-pmap-c)# <b>exit</b>	(Optional) Exits policy-map class configuration mode.

Traffic policy can be nested with another traffic policy using the **service-policy** command, called as **Hierarchical traffic policy**. The policy which holds another policy is the parent policy and the nested one is called child policy.

**Sample configuration of policy with parent-child relationship:**

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# exit
```

## User Management

The **User Management** option lets you manage different users with varying access privileges. You can assign different users to different device groups and IP groups, and allow them to manage the assigned groups exclusively. You can choose from three types of users in NetFlow Analyzer - Administrator, Operator, and Guest. You can create any number of users of each type, and assign them to any number of device groups and IP groups.

The administrative privileges for each user are described below:

Privilege	Administrator	Operator	Guest
View all available devices and IP groups	✓	✗	✗
Create, modify, or delete device groups or IP groups	✓	✗	✗
Modify Runtime Administration properties	✓	✗	✗
Change other users' passwords	✓	✗	✗
Manage licensed interfaces	✓	✗	✗
Apply different licenses	✓	✗	✗
Create other Administrator users	✓	✗	✗
Create other Operator users	✓	✗	✗
Create other Guest users	✓	✓ *	✗
Add, modify, or delete Alerts	✓	✓ **	✗
Enabling and Disabling Alerts	✓	✓ ***	✗
Add, modify, or delete applications	✓	✓	✗
Change device settings	✓	✓	✗
View traffic reports	✓	✓	✓
View custom reports	✓	✓	✓
Assigned to one or more device groups or IP groups	✗	✓	✓
Scheduling of Reports	✓	✗	✗
NBAR Configuration	✓	✗	✗
Viewing NBAR Reports	✓	✓	✓

\* only within the assigned group

\*\* It is not possible to delete a Link Down Alert

\*\*\* Link Down alert can be enabled or disabled only by Administrator


### Adding a New User

On the User Management page, click the **Add** button to add a new user. Fill in the following fields and click the **Add User** button to create this user.


Field	Description
User Name	Enter the unique user name for the user. This name will be used to log in to the NetFlow Analyzer web client.
Password, Retype Password	Enter a password for this user. The password should be at least 6 characters long, and all characters are allowed.
Access Level	Select the Access Level for the user. Remember that access levels will be available depending on your own access permissions. For example, if you have logged in as an Administrator, all three access levels will be available in the Access Level options box.
Available Groups	Select the device groups to assign to this user and move them to the Selected Groups.
Available IP Groups	Select the IP groups to assign to this user and move them to the Selected IP Groups.

Click on the user name at any time on the **User Management** page to view the corresponding user name, access level, and assigned device groups and IP groups.


## Changing User Passwords


Only an Administrator user can reset the password of any other user. To assign a new password to a user, click on the  icon or the **Assign New** link.

Enter a new password, confirm it, and click the **Update** button for the new password to take effect.

	If you have logged in as an Admin user, you can change your own password in the same way as described above. If you have logged in as an Operator user or a Guest user you can change your password by selecting the Change Password option in the <b>Admin Operations</b> menu.
--	--


## Editing User Details

Click on the  icon against a user, to edit the user's details.

	You can only modify the device groups and IP groups which have been assigned to the user. You <b>cannot</b> modify the user name or the access level, irrespective of your own access level.
---	--

Once you are done, click the **Update** button to save your changes.

## Deleting a User

Click the  icon against a user name to delete the respective user. Once a user is deleted, all details of this user are permanently deleted.

## License Management

---

The **License Management** option lets you manage the interfaces exporting NetFlow data to NetFlow Analyzer, depending on the license that you have purchased.



The options visible under the **Admin Operations** menu depend on the user level you have logged in as. Look up User Management to know more about user levels and the respective admin operations allowed.

The status box at the top of the page indicates the type of license currently applied, the total number of interfaces currently managed, and the number of days remaining for the license to expire.

Look up Licensing to know more about upgrading your license.

The Router List shows all the routers and interfaces from which NetFlow exports are received, and whether they are managed or not.

### Managing a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Once you have selected the required interfaces, click the **Manage** button to manage these interfaces. This means that flows received from these interfaces will be processed by NetFlow Analyzer, and traffic graphs and reports can be generated.

The maximum number of interfaces that can be managed, depends on the current license applied.

### Unmanaging a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Unmanage** button to unmanage these interfaces. This means that flows received from these interfaces will be dropped by NetFlow Analyzer. Once unmanaged, these interfaces will not be seen on the Dashboard or be listed in device groups. However they will still be listed in the Router List in the License Management page.

### Deleting a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Delete** button to delete these interfaces. This means that these interfaces are completely removed from all screens of the NetFlow Analyzer client.

However, if flows are still being sent from these interfaces to NetFlow Analyzer, they will reappear in the Dashboard. To prevent this, you need to disable NetFlow export from those interfaces.

### Licensing New Interfaces

If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is less than that allowed in the current license, this interface is listed under Router List on the Dashboard with a message saying new flows have been received. You need to then click the **License Management** option and change this interface's status to Managed in order to include this interface in the list of managed interfaces, and also generate traffic graphs and reports for the same.

If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is equal to that allowed in the current license, you need to either unmanage any other managed interfaces, and then manage this interface, or leave this interface in **New** status. In any case graphs and reports can be generated only for managed interfaces.

At any time you can buy more licenses by clicking on the **Buy Online** image.

## Change Password

---

The **Change Password** option lets you change your own password for logging in to NetFlow Analyzer. This is available as a separate option in the Admin Operations menu, for users logged in as Operator or Guest. For Admin users, the password can be changed from the User Management page itself.

Enter the new password, confirm it, and click the **Update** button to save your changes.



Enter the new password when you log in again into NetFlow Analyzer. Your present session will not be terminated until you explicitly log out or your session expires.

## **NetFlow Analyzer Add-on**

---

Add-on is an integrated part of NetFlow Analyzer and the license for the Add-on has to be applied separately. NetFlow Analyzer has the following Add-on:

- VoIP Monitor

# VoIP Monitor

## About VoIP Monitor

---

Cisco IPSLA monitor or VoIP monitor comes as an add-on feature in NetFlow Analyzer and requires license to run. NetFlow Analyzer continuously monitors the key performance metrics of the VoIP network to determine its health. The parameters measured include Jitter, Latency, Packet Loss etc.

**Jitter:** Jitter indicates a variation in delay between arriving packets (inter-packet delay variance). Users often experience uneven gaps in speech pattern of the person talking on the other end, and sometimes there are disturbing sounds over a conversation coupled with loss of synchronization etc.

**Latency:** The delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site is called as latency. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

**Packet Loss :** Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency.

**MOS:** The jitter codec determines the quality of VoIP traffic and each codec provides a certain quality of speech. The Mean Opinion Score is a standard for measuring voice codecs and is measured in the scale of 1 to 5 (poor quality to perfect quality). The quality of transmitted speech is a subjective response of the listener.

## How it works

NetFlow Analyzer primarily relies on Cisco's IP-SLA for monitoring the VoIP and the prerequisite therefore is, that the device should be a Cisco Router and must have IPSLA agent enabled on it. From IOS Version 12.3(14)T all Cisco routers support monitoring of VoIP QoS metrics.

Cisco's IPSLA, an active monitoring feature of Cisco IOS software, facilitates simulating and measuring the above mentioned parameters to ensure that your SLAs are met.

Cisco IP SLA provides a UDP jitter operation where UDP packets are sent from the source device to a destination device. This simulated traffic is used to determine the jitter, the round-trip-time, packet loss and latency. This data is gathered for multiple tests over a specified period to identify how the network performs at different times in a day or over a few days. The VoIP monitor gathers useful data that helps determine the performance of your VoIP network, equipping you with the required information to perform network performance assessment, troubleshooting, and continuous health monitoring.

## Adding a New VoIP Monitor

---

### Prerequisites

When you want to test a link from your office to another location, you need a Cisco router ( IOS version 12.4 or later ) at each end.

### Steps to set up the monitor

Using NetFlow Analyzer, you can now monitor the voice and video quality of a 'call path'. Call path is the WAN link between the router in your main office and the one in the branch office that you want to monitor.

**Step 1 :** Export NetFlow from the router in your LAN to NetFlow Analyzer. And make sure the SNMP read and write community are configured properly, for that router.

**Step 2:** Enable SLA responder on the destination device you wish to monitor, Steps are detailed below.

- Open a CLI session on the destination router and enable the EXEC mode as follows:  
**Router>enable**
- Start the global configuration mode:  
**Router#configure termina**
- Enable the IP SLA responder:  
**Router(config)#ip sla responder**  
[or]  
**Router(config)#ip sla monitor responder**  
(Note: Enter any one of the command to enable IP SLA responder as it varies according to the IOS versions.)
- Repeat the above steps for all the destination routers on which you want to monitor VoIP performance.

**Step 3:** Creating the VoIP monitor:

- Go to Modules-> VoIP Monitors->Configure VoIP Monitor-> Create New, and enter a name for the monitor.
- Select the source router from the list of routers discovered in NetFlow Analyzer, and select the relevant interface.
- Specify the destination router either by using the 'Search' option to pick from the discovered routers, or use the 'Add' option to specify the IP address of the destination router and submit the details.
- You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure. Refresh the page after few seconds to see the new monitor. The data will be collected every hour, from the time you have configured.

[or]

You can also create the VoIP monitor from the Router snapshot page. To do so, go to Router snapshot page, click on Action tab and select Add VoIP Monitor. Enter the Monitor Name and Destination IP. Click Submit to create the monitor or Click Advanced button to go to Create New VoIP Monitor page and follow the steps from b to d given under Step 3.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds ( default value). NetFlow Analyzer updates this statistics (collected data) every hour and the reports are generated after one hour of configuration. Go through the FAQs section to understand QoS parameters.

## Configuring call settings and threshold template

---

### Defining Call Settings:

Define a template with the required VoIP settings to be used for monitoring performance. The VoIP template comes with pre-populated default values. In case you would like to effect some changes to the values before initiating monitoring, make the changes as follows:

1. Go to Modules and click VoIP Monitors.
2. Go to Settings-> Call Settings.
3. Configure the following parameters:

**Destination Port** - Specify the VoIP UDP port to which VoIP Monitor sends simulated traffic to generate performance metrics. The default port number is set as 16384. You can specify a port in the range of 16384 - 32766.

**Simulated VoIP Codec** - The VoIP jitter codec decides the type of traffic that VoIP Monitor simulates over your network.

**Operation Frequency** - The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.

**Operation Timeout** - The operation timeout is time to wait for the response from the responder / destination device in msec.

**Type of service** - The Type of Service octet allows you to set precedence levels for VoIP traffic of the IP SLA operations.

**MOS Advantage Factor** - The advantage factor is a measure, on a scale of 0 to 20, of the willingness of your VoIP network users to trade call quality for convenience.

### Defining Thresholds for the monitored parameters:

You can define a threshold template so that the VoIP performance parameters can be better suited to your company SLA's (Service Level Agreements). Alerts are triggered based on the thresholds configured so that you can take corrective actions in time. Here are the steps to define a threshold template:

1. Go to Modules and click VoIP Monitors.
2. Go to Settings->Threshold Template.
3. Configure the following values:

**MOS Threshold** : Configure the MOS threshold by specifying the upper and lower MOS range values in the range of 1 to 5.

**Jitter Threshold** : Configure the jitter threshold in msec with upper and lower threshold limits. The range is from 0 to 6000 msec.

**Latency Threshold** : Specify the delay allowed in msec again in the range of 0 to 6000.

**Packet Loss** : Specify the number of packets that can be lost in transit.

**Notification Profile** : Select the required notification profile(s) in order to notify when any threshold rule is violated.

## Viewing Top 10 Call Paths

---

With VoIP Monitor you can view the top 10 call paths by MOS, Packet Loss, Jitter and Latency. This provides you to have a quick view and react proactively. To view the top 10 call paths, follow the steps given below:

1. Go to Modules and click on **VoIP Monitors**.
2. Click on **Top 10**. The top 10 call paths by MOS, Packet Loss, Jitter and Latency are listed.
3. Click on the required call path view its snapshot page.

## FAQs on VoIP Monitor

---

1. Why do i need to set SNMP write community on the Source Router ?
2. Why I am getting 'Source router SNMP write community may be wrong' error message?
3. Why should the SLA Responder be enabled on the destination device ?
4. Why are the VoIP metrics shown as zero or 'Not available' in NetFlow Analyzer?
5. What are all the VoIP QoS metrics measured by NetFlow Analyzer ?
6. How do i choose the codec ?
7. How much bandwidth does each monitor occupy ?

### 1. Why do i need to set SNMP write community on the Source Router ?

Both, the SNMP read and write community string needs to be set on the source router. The write community is used to configure the IPSLA on the device while the read community is used by NetFlow Analyzer to gather performance data from the router.

### 2. Why I am getting 'Source router SNMP write community may be wrong' error message?

NetFlow Analyzer uses SNMP to gather data from the Cisco IP SLA agent. This error is displayed when wrong SNMP read / write community string is configured for the Source router of the VoIP Monitor in NetFlow Analyzer.

To configure the correct SNMP write community string in NetFlow Analyzer, go to the snapshot page of the source router and change the SNMP credentials by clicking on the '**Click here to change**' corresponding to the "**Passwords**" field. In the pop-up enter the appropriate credentials and submit it. After successfully submitting the correct SNMP credentials, try to add the VoIP Monitor again for the Source device (Modules > VoIP Monitor > Settings).

### 3. Why should the SLA Responder be enabled on the destination device ?

Enabling the IP SLAs Responder provides the details of packet loss statistics on the device sending IP SLAs operations. IP SLAs Responder is enabled on the target router (rtr responder) before configuring a Jitter operation.

### 4. Why are the VoIP metrics shown as zero or 'Not available' in NetFlow Analyzer?

You will see zero or 'not available' values when data is not collected for the monitored metrics. This can be either due to incorrect SNMP read community configured, or of the Responder is not enabled on the destination device. Make sure that the correct SNMP read community is configured and the SLA Responder is enabled.

### 5. What are the critical parameters monitored to determine the VoIP QoS performance?

The monitored parameters include Latency, Jitter, Packet Loss, and MOS. The parameters are described below for reference:

**Jitter** : Jitter is defined as a variation in the delay of received packets. Users often experience disturbing sounds over a conversation coupled with loss of synchronization at times and is referred to as jitter. High levels of jitter can result in some packets getting discarded and thereby impact the call quality. Ensuring a jitter-free transmission to provide qualitative service depends on identifying the bottle-neck responsible for the jitter, and acting on it to eliminate it. NetFlow Analyzer's VoIP monitoring feature helps you find the problem and ensures maximum QoS on your VoIP network.

**Packet Loss** : Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency. Using NetFlow Analyzer, you can monitor the packet loss and take corrective actions based on the information.

**One way Latency:** Latency (delay) is the time taken for a packet to reach the destination device. When monitoring latency over VoIP, the delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

**Round Trip Time:** Round Trip Time is the time taken for a packet to reach the destination and again comes back to the source device. The total time it takes for the round trip is measured in milliseconds.

**MOS:** The Mean Opinion Score is the key quality indicator of VoIP traffic quality. And is measured in the scale of 1 to 5 (poor to excellent quality). [back to top]

## 6. What is VoIP codec?

Codecs (Coder/Decoder) serve to encode voice/video data for transmission across IP networks. The compression capability of a codec facilitates saving network bandwidth and it is therefore appropriate that you choose the correct codec for your IP network. Here is a quick reference to the codecs with the corresponding packets size and bandwidth usage:

Codec & Bit Rate (Kbps)	Operation Frequency	Default number of packets	Voice Payload Size	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711a/u (64 kbps)	60 msec by default. You can specify in the	1000	160 + 12 RTP bytes	82.8 kbps	67.6	87.2
G.729 (8 kbps)	range of 0 - 604800 msec.	1000	20 + 12 RTP bytes	26.8 kbps	11.6	31.2

## 7. How much bandwidth does each monitor occupy ?

The bandwidth occupied depends on the codec selected. Look at the above table for reference. [back to top]

## Contacting Technical Support

---

Click the **Support** link on the top-left corner of the NetFlow Analyzer client screen, to see a wide range of options to contact the NetFlow Analyzer Technical Support team in case of any problems.

Option	Description
Request Technical Support	Click this link to submit a form from the NetFlow Analyzer website, with a detailed description of the problem that you encountered
Create Support Information File	Click this link to create a ZIP file containing all the server logs that the Technical Support team will need to analyze your problem. You can then send this ZIP file to netflowanalyzer-support@manageengine.com or upload it to our server via FTP.
Troubleshooting Tips	Click this link to see troubleshooting tips for common problems encountered by users.
User Forums	Click this link to go to the NetFlow Analyzer user forum. Here you can discuss with other NetFlow Analyzer users and understand how NetFlow Analyzer is being used across different environments
Need a Feature	Click this link to submit a feature request from the NetFlow Analyzer website
Toll-free Number	Call the toll-free number <b>+1 888 720 9500</b> to talk to the NetFlow Analyzer Technical Support team directly

## Frequently Asked Questions

---

### Installation

1. When I try to access the web interface, another web server comes up. How does this happen?
2. How can I change the MySQL port in NetFlow Analyzer from 13310 to another port?
3. Can I install and run NetFlow Analyzer as a root user?
4. Is a database backup necessary, or does NetFlow Analyzer take care of this?
5. How do I update patch in Linux ?

### Router Configuration

1. Why can't I add a router to NetFlow Analyzer?
2. My router has been set up to export NetFlow data, but I still don't see it on the Dashboard.
3. I've deleted a router and all its interfaces through the License Management page but it still comes up on the Dashboard.
4. What's the difference between unmanaging and deleting an interface?
5. How to Configure SNMP community in router?
6. How do I set the router time in SYNC with the NFA server?

### Reporting

1. The graphs are empty
2. What is Aggregate data and Raw data ? How to set Raw data ?
3. Some of the applications are labeled as "TCP\_App" or something similar. What is that?
4. Why are only the top 5 or 10 values shown in the reports? What if I want more detail?
5. The graphs show only IN traffic for an interface, although there is both IN and OUT traffic flowing through that interface. Why's that?
6. Why are some interfaces labeled as IfIndex2, IfIndex3, etc.?
7. The total bandwidth usage seems to decrease depending on the length of the report. Why is that?

### NBAR

1. Which features are not supported by NBAR?
2. Any restrictions on where we can configure NBAR?
3. What Does NBAR Performance Depend On?
4. Is performance dependent on the number of interfaces that NBAR is enabled on? Does the link speed of the interface(s) that NBAR is enabled?
5. I am able to issue the command "ip nbar protocol-discovery" on the router and see the results. But NFA says my router does not support NBAR, Why?
6. How do I verify whether my router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB?

### V9

1. What is NetFlow Version 9?
2. What is the memory impact on the router?
3. "Receiving non V5/V7/V9 packets from the following devices: Click here for further details.." What does this mean?
4. Is version 9 backward compatible ?

5. What is the performance impact of V9?
6. What are the restrictions for V9?
7. How do I configure NetFlow Version 9?

## Technical Information

1. How is traffic information stored in the NetFlow Analyzer database?
2. How do I reset the admin password ?
3. How are ports assigned as applications in NetFlow Analyzer?
4. Do I have to reinstall NetFlow Analyzer when moving to the fully paid version?
5. How many users can access the application simultaneously?
6. NetFlow Analyzer logs out after a period of inactivity. How do I avoid that?
7. How to create DBInfo log file ?
8. Why the interface shows 100% utilization ?
9. What information do I need to send to NFA support for assistance?
10. How to safely migrate NFA installation to different machine ?
11. What do I do if my NFA server becomes slow ? (or) How do I improve my NFA system performance ?
12. Why NFA says router time not is SYNC and stops collecting data ?

## Installation

1. **When I try to access the web interface, another web server comes up. How does this happen?**

During installation, NetFlow Analyzer checks if the selected port is in use by another application. If at that time, the other webserver was down, it will not get detected. Either disable the other web server, change its server port, or change the NetFlow Analyzer web server port.

2. **How can I change the MySQL port in NetFlow Analyzer from 13310 to another port?**

Edit the mysql-ds.xml file in the /server/default/deploy directory. Change the port number in the line to the desired port number, save the file, and restart the server.

3. **Can I install and run NetFlow Analyzer as a root user?**

NetFlow Analyzer can be installed and started as a root user, but all file permissions will be modified and later you cannot start the server as any other user.

4. **Is a database backup necessary, or does NetFlow Analyzer take care of this?(or)How to back-up data in NetFlow Analyzer ?**

NetFlow Analyzer includes a database backup utility that you can use to make a backup of the database. There are 2 ways of backup :

1. You can execute the script "backupdb.bat" / "backupdb.sh" which can be found under \$NETFLOW\_HOME/troubleshooting. This will create a backup of the database in a zip format. When you want to restore. You have to extract the zip to the \$NETFLOW\_HOME directory. This is a slow process.
2. You can copy the folder \$NETFLOW\_HOME/mysql/data to a different location and to restore you can copy it back to the same location. This is a fast process.

- In both the above process the version of NFA should be the same.

#### How do I update patch in Linux ?

Please use the command "**sh UpdateManager.sh -c**" and follow the instructions to upgrade NetFlow Analyzer.

## Router Configuration

- Why can't I add a router to NetFlow Analyzer?**

NetFlow Analyzer does not choose which routers or interfaces to monitor. Devices are auto-discovered. All you need to do is set up your interfaces to send NetFlow data to the specified port on NetFlow Analyzer. Once NetFlow Analyzer starts receiving NetFlow data, you can see the device and its interfaces listed on the Dashboard.

- My router has been set up to export NetFlow data, but I still don't see it on the Dashboard.**

There are a number of things you can check here:

- Check if NetFlow is enabled on the device, and that it has started sending flows.
- Check if your router is exporting NetFlow data to the port on which NetFlow Analyzer is listening.
- Check if the router is exporting NetFlow version 5 data. Flows with any other version will be discarded.

- I've deleted a router and all its interfaces through the License Management page but it still comes up on the Dashboard.**

This happens because NetFlow packets are still being received from that router. Unless you configure the router itself to stop exporting NetFlow data to NetFlow Analyzer it will reappear on the Dashboard

- What's the difference between unmanaging and deleting an interface? (or) When do I unmanage a device and when do I delete it from the License Management page?**

If you need to temporarily stop monitoring a router/interface, unmanage it from License Management. In this case, the router/interface is still shown under License Management. If you need to permanently stop monitoring a router/interface, disable NetFlow exports from the interface/router and then delete it from License Management. In this case, the router/interface is not displayed on any of the client screens unless new flows are sent from it.

- How to Configure SNMP community in router?**

For configuring SNMP, follow the steps below

- Logon on to the router.
- Enter into the global configuration mode
- Type the command `snmp-server community public RO` ( to set public as Read-Only community )
- Press ctrl and Z
- Type the command `write mem`

- **How do I set the router time in SYNC with the NFA server?**

Whenever the time difference between the NetFlow Analyzer Server and the router is above 10 minutes a warning icon will appear in the home page. When this happens, NetFlow Analyzer will stamp the flows based on the system time of the NetFlow Analyzer server. In case you see this, please ensure the following on the router:

1. Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the configure terminal and typing **show running-config**. You can set the clock time zone and offset using the command `clock timezone zone hours [minutes]` (E.g. **clock timezone PST -8 00**)

2. After checking the time zone, check if the correct time is set on your router. You can check this by logging into the router and typing `show clock`. You can set the clock time using the command **clock set hh:mm:ss date month year**. [ A sample - **clock set 17:00:00 27 March 2007**] There is no queueing mechanism done on heavy periods.

## Reporting

1. **The graphs are empty**

Graphs will be empty if there is no data available. If you have just installed NetFlow Analyzer, wait for at least ten minutes to start seeing graphs. If you still see an empty graph, it means no data has been received by NetFlow Analyzer. Check your router settings in that case.

2. **What is Aggregate data and Raw data ? How to set Raw data ?**

As far as aggregated data is concerned, NetFlow Analyzer maintains the top 'n' flows for every ten minutes slot. The record count determines this 'n' values. By default it is set to 50. You may set your own criteria for this purpose. you can change this from the Settings option.

Apart from this NetFlow Analyzer allows you to store raw data (all flows -not just the top n) for upto one month.

1. Aggregated data is stored in 5 levels of tables - 10 Min, Hourly, 6 Hour, 24 Hour and Weekly tables and reports for different periods need to access the corresponding table. For example, very recent reports need to access the 10 Min table and old reports need to access the Weekly table. You can access the table MetaTable to determine the table which contains data for the required time period.
2. Raw data is stored in dynamically created tables and data pertaining to different devices (routers) reside in different table for different periods of time. You can access the table RawMetaTable to determine the table which contains data for the required report.

3. **Some of the applications are labeled as "TCP\_App" or something similar. What is that?**

If an application is labeled as "TCP\_App" or something similar, it means that NetFlow Analyzer has not recognized this application (i.e.) the combination of port and protocol is not mapped as any application. Once you add these applications under Application Mapping they will be recognized.


**4. Why are only the top 5 or 10 values shown in the reports? What if I want more detail?**

NetFlow Analyzer shows the top 50 results in all reports by default. You can see up to 100 results in each report by changing the Record Count value in the Settings page.

**5. The graphs show only IN traffic for an interface, although there is both IN and OUT traffic flowing through that interface. Why's that?**

Check if you have enabled NetFlow on all interfaces through which traffic flows. Since NetFlow traffic accounting is ingress by default, only IN traffic across an interface is accounted for. To see both IN and OUT traffic graphs for an interface, you need to enable NetFlow on all the interfaces through which traffic flows.

**6. Why are some interfaces labeled as IfIndex2, IfIndex3, etc.?**

This happens if the device/interface has not responded to the SNMP requests sent by NetFlow Analyzer. Check the SNMP settings of the interface or manually edit the interface name from the Dashboard. NetFlow Analyzer uses port 161, and the *public* community string as default SNMP values. If the SNMP settings of your device are different, click the  icon next to the device/interface in the Dashboard Interface View to change the values. If you need to change this globally, enter the new values in the same fields under Settings.]

**7. The total bandwidth usage seems to decrease depending on the length of the report. Why is that?**

NetFlow Analyzer aggregates older data in less granular format and due to this reason some of the spikes may not show in older reports. While reports pertaining to last day is generated from tables with 10 minute granularity, reports pertaining to last week is generated from tables with 1 hour granularity

For example, data in 10 minute table pertaining to 10:00, 10:10, 10:20, 10:30, 10:40 and 10:50 would all be aggregated and moved into hourly data tables for one data point pertaining to 10:00.

While the total data volumes is correct, the traffic rates will be averaged over this period. So:

10:00 -> volume transferred 100MBytes, ten minute average rate 1,333Kbits/s  
 10:10 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s  
 10:20 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s  
 10:30 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s  
 10:40 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s  
 10:50 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s

When aggregated into the one hour table, we get:

10:00 -> volume transferred 105MBytes, one hour average rate 233Kbits/s

The spike up to 1,333Kbits/s has been lost by this averaging process; as the data get aggregated into longer and longer time periods, so this average value will decrease further.

This is the reason for the reduction in the reporting of bandwidth usage over time.

## NBAR

### 1. Which features are not supported by NBAR ?

The following features are not supported by NBAR:

- More than 24 concurrent URLs, HOSTs or MIME type matches
- Matching beyond the first 400 bytes in a URL
- Non-IP traffic
- Multicast and other non-CEF switching modes
- Fragmented packets
- Pipelined persistent HTTP requests
- URL/HOST/MIME/ classification with secure HTTP
- Asymmetric flows with stateful protocols
- Packets originating from or destined to the router running NBAR

### 2. Any restrictions on where we can configure NBAR?

You can't configure NBAR on the following logical interfaces:

- Fast EtherChannel
- Interfaces that use tunneling or encryption
- VLANs
- Dialer interfaces
- Multilink PPP

**Note:** NBAR is configurable on VLANs as of Cisco IOS Release 12.1(13)E, but supported in the software switching path only.

### 3. What Does NBAR Performance Depend On?

Several factors can impact NBAR performance in software-based execution.

#### A. Router Configuration

1. Number of protocols being matched against it
2. Number of regular expressions being used
3. The complexity of packet inspection logic required

#### B. Traffic Profile (Packet Protocol Sequence)

1. The number of flows
2. Long duration flows are less expensive than shorter duration flows
3. Stateful protocol matches are more performance impacting than static port applications

### 4. Is performance dependent on the number of interfaces that NBAR is enabled on? Does the link speed of the interface(s) that NBAR is enabled on affect performance ?

No. NBAR performance is not dependent on the number of interfaces that NBAR is enabled on or the link speed of those interfaces. Performance is dependent on the number of packets that the NBAR engine has to inspect, how deep into the packet it has to look to perform regular inspection.

**5. I am able to issue the command "ip nbar protocol-discovery" on the router and see the results. But NFA says my router does not support NBAR, Why?**

Earlier version of IOS supports NBAR discovery only on router. So you can very well execute the command "ip nbar protocol-discovery" on the router and see the results. But NBAR Protocol Discovery MIB(CISCO-NBAR-PROTOCOL-DISCOVERY-MIB) support came only on later releases. This is needed for collecting data via SNMP. Please verify that whether your router IOS supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB.

**5. How do I verify whether my router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB?**

a) You can check CISCO-NBAR-PROTOCOL-DISCOVERY-MIB supported platforms and IOS using the following link.

<http://tools.cisco.com/ITDIT/MIBS/AdvancedSearch?MibSel=250073>

b) Alternately , you can execute "show snmp mib | include cnpd " command at router to know the implemented mib objects in the router. If the router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB, then the above command gives the following objects.

```
cnpdStatusEntry.1
cnpdStatusEntry.2
cnpdAllStatsEntry.2
cnpdAllStatsEntry.3
cnpdAllStatsEntry.4
cnpdAllStatsEntry.5
cnpdAllStatsEntry.6
cnpdAllStatsEntry.7
cnpdAllStatsEntry.8
cnpdAllStatsEntry.9
cnpdAllStatsEntry.10
cnpdAllStatsEntry.11
cnpdAllStatsEntry.12
cnpdTopNConfigEntry.2
cnpdTopNConfigEntry.3
cnpdTopNConfigEntry.4
cnpdTopNConfigEntry.5
cnpdTopNConfigEntry.6
cnpdTopNConfigEntry.7
cnpdTopNConfigEntry.8
cnpdTopNStatsEntry.2
cnpdTopNStatsEntry.3
cnpdTopNStatsEntry.4
cnpdThresholdConfigEntry.2
cnpdThresholdConfigEntry.3
cnpdThresholdConfigEntry.4
cnpdThresholdConfigEntry.5
cnpdThresholdConfigEntry.6
cnpdThresholdConfigEntry.7
cnpdThresholdConfigEntry.8
cnpdThresholdConfigEntry.9
cnpdThresholdConfigEntry.10
cnpdThresholdConfigEntry.12
```

cnpdThresholdHistoryEntry.2  
 cnpdThresholdHistoryEntry.3  
 cnpdThresholdHistoryEntry.4  
 cnpdThresholdHistoryEntry.5  
 cnpdThresholdHistoryEntry.6  
 cnpdThresholdHistoryEntry.7  
 cnpdNotificationsConfig.1  
 cnpdSupportedProtocolsEntry.2

## V9

### 1. What is NetFlow Version 9?

This format is flexible and extensible, which provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as NAT, MPLS, BGP next hop and Multicast. The main feature of Version 9 Export format is that it is template based.

### 2. What is the memory impact on the router due to V9?

The memory used depends upon the data structures used to maintain template flowsets. As the implementation does not access the NetFlow cache directly the memory used is not very high.

### 3. "Receiving non V5/V7/V9 packets from the following devices: Click here for further details.." What does this mean?

If you get this message on the user interface, it means that NetFlow packets with versions other than version 5/7/9, are being received by NetFlow Analyzer. Check your router settings to make sure that **only** version 5/7/9 NetFlow exports are being sent to NetFlow Analyzer. This is because NetFlow Analyzer supports only NetFlow version 5/7/9 exports.

### 4. Is version 9 backward compatible ?

Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, then you must configure Version 5 or Version 8.

### 5. What is the performance impact of V9?

Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets requires additional processing.

### 6. What are the restrictions for V9?

Version 9 allows for interleaving of various technologies. This means that you should configure Version 9 if you need data to be exported from various technologies (such as Multicast, DoS, IPv6, BGP next hop, and so on).

### 7. How do I configure NetFlow Version 9?

Please refer the following document for configuring netflow version 9

[http://www.cisco.com/en/US/products/ps6350/products\\_configuration\\_guide\\_chapter09186a00805e1b4a.html](http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e1b4a.html)

## Technical Information

### 1. How is traffic information stored in the NetFlow Analyzer database?

For each report, NetFlow Analyzer stores traffic information in a different manner. The following tables describe the data storage pattern for the various reports generated by NetFlow Analyzer.

Data storage pattern		
Granularity	Traffic Tables (SRC & DST)	Application, Source, Destination and Conversation
10Min	30 hours	25 hours
Hourly	32 Days	32 Days
6 Hour	32 Days	32 Days
24 Hour	92 Days	90 Days
Weekly	forever	forever

Reports for last day		
Time Period	Traffic Tab	Application, Source, Destination and Conversation
Last 24 hour period	1 minute granularity	hourly granularity
Less than 6 hour interval	1 minute granularity	10 minute granularity
Less than 2 hour interval	1 minute granularity	1 minute granularity

Reports for last week		
Time Period	Traffic Tab	Application, Source, Destination and Conversation
Last 7 days	hourly granularity	6 hour granularity
Less than 12 hour interval	1 minute granularity	hourly granularity
Less than 2 hour interval	1 minute granularity	1 minute granularity ( if no raw table is available goes to hourly granularity )

Reports for last month		
Time Period	Traffic Tab	Application, Source, Destination and Conversation
Last 30 days	hourly granularity	6 hour granularity
Less than 24 hour interval	1 minute granularity	hourly granularity
Less than 2 hour interval	1 minute granularity	1 minute granularity ( if no raw table is available goes to hourly granularity )

Reports for last quarter		
Time Period	Traffic Tab	Application, Source, Destination and Conversation
Last quarter	24 hour granularity	24 hour granularity
Less than 24 hour interval (beyond last 30 days)	1 minute granularity	24 hour granularity

### 2. How do I reset admin password?

Please ensure that the server is running before doing the below steps:

1. Open a command prompt
2. Go to the \mysql\bin directory
3. Type `mysql -u root --port=13310`
4. Type `use netflow`
5. Execute the following query:  

```
update AaaPassword, AaaLogin, AaaAccount, AaaAccPassword
setAaaPassword.PASSWORD='Ok6/FqR5WtJY5UCLrnvjQQ==',
AaaPassword.SALT='12345678' where AaaLogin.LOGIN_ID = AaaAccount.LOGIN_ID
and AaaAccount.ACCOUNT_ID =AaaAccPassword.ACCOUNT_ID and
AaaPassword.PASSWORD_ID =AaaAccPassword.PASSWORD_ID and
AaaLogin.NAME = 'admin' ;
```
6. Type `quit` to quit mysql

7. Type exit to exit command prompt
8. Login as admin / admin. You can change the password again if you wish.

### 3. How are ports assigned as applications in NetFlow Analyzer?

A NetFlow export contains information on the protocol, source port, and destination port. When a flow is received, NetFlow Analyzer tries to match the port and protocol in the flow, to an application in the following order:

1. The smaller of the source and destination port numbers, to the list of ports configured to each application in the Application Mapping list
2. The larger of the source and destination port numbers, to the list of ports configured to each application in the Application Mapping list
3. The smaller of the source and destination port numbers, to the port ranges configured to each application in the Application Mapping list
4. The larger of the source and destination port numbers, to the port ranges configured to each application in the Application Mapping list

If a matching application is still not found, then depending on the protocol received in the flow, the application is listed as **<protocol>\_App**. (eg.) TCP\_App if a flow is received with TCP protocol, and unmatched source and destination ports. If the protocol received in the flow is also not recognized by NetFlow Analyzer, the application is listed as **Unknown\_App**.



A single flow can be categorized as a single application only. In case of a conflict, applications with an exact match for the port number will be accounted for.

### 4. Do I have to reinstall NetFlow Analyzer when moving to the fully paid version?

No, you do not have to reinstall or shut down the NetFlow Analyzer server. You just need to enter the new license file in the Upgrade License box.

### 5. How many users can access the application simultaneously?

This depends only on the capacity of the server on which NetFlow Analyzer is installed. The NetFlow Analyzer license does not limit the number of users accessing the application at any time.

### 6. NetFlow Analyzer logs out after a period of inactivity. How do I avoid that?

You can change the time-out value to a higher value than the default ( 30 minutes ) by increasing the parameter **session-timeout**.

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

under **<NFA\_Home>/AdventNet/ME/NetFlow/server/default/conf/web.xml**

Change the value 30 to your desired time-range - say, 600. You will have to restart NFA server for this to take effect.

### 6. How to create DBInfo log file ?

1. Please ensure that NFA is running.
2. Navigate to /Troubleshooting directory and execute the file DBInfo.sh / DBInfo.bat
3. It creates a "Info.log" file in the same folder. Please send us the "info.log" file.

### 8. Why the interface shows 100% utilization ?

Please refer this link for a brief explanation of 100% utilization:

<http://forums.manageengine.com/?ftid=49000002654747>

8. What information do I need to send to NFA support for assistance?
  1. Please run your logziputil.bat / logziputil.sh (under the troubleshooting folder). This will create a zip file under the support folder please send us the zip file.
  2. Send us the .err file under the Mysql\data folder.
  3. Also send your Machine configuration.

8. How to safely migrate NFA installation to different machine ?

Please follow the steps below to move your installation,

1. Copy the data folder in /mysql folder of the installation that you wish to move, to a safe location.
  2. Install NetFlow Analyzer in the new location, start it once and shut it down.
  3. Replace the data folder in /mysql folder of the new installation with the data folder of the old installation.
  4. Start NetFlow Analyzer.
9. **What do I do if my NFA server becomes slow ? (or) How do I improve my NFA system performance ?**

Please refer this link for a brief note on database tuning  
:http://forums.manageengine.com/?ftid=49000002654617

#### **Why NFA says router time not is SYNC and stops collecting data ?**

Please follow these steps to fix this issue:

- In case you see this, please ensure the following on the router: Check if the correct time is set on your router.  
You can check this by logging into the router and typing **show clock**. You can set the clock time using the command **clock set hh:mm:ss month date year**. Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the **configure terminal** and typing **show running-config**. You can set the clock time zone and offset using the command **clock timezone zone hours [minutes]** (E.g. clock timezone PST -8 00)
- The time sync issue may be related to high CPU load and reducing the IP group can help. Each address / range / network will be checked separately. So, 4 addresses of 10.10.10.1, 10.10.10.2, 10.10.10.3 and 10.10.10.4 will add more overload than creating the same as a single IP range of 10.10.10.1 to 10.10.10.4. While associating interfaces you are better off selecting "All interfaces" wherever appropriate since in that case no check will be done with the interface in the flow. In your case, since you had 180 interfaces associated, the code had to check for these 180 interfaces in each flow received.

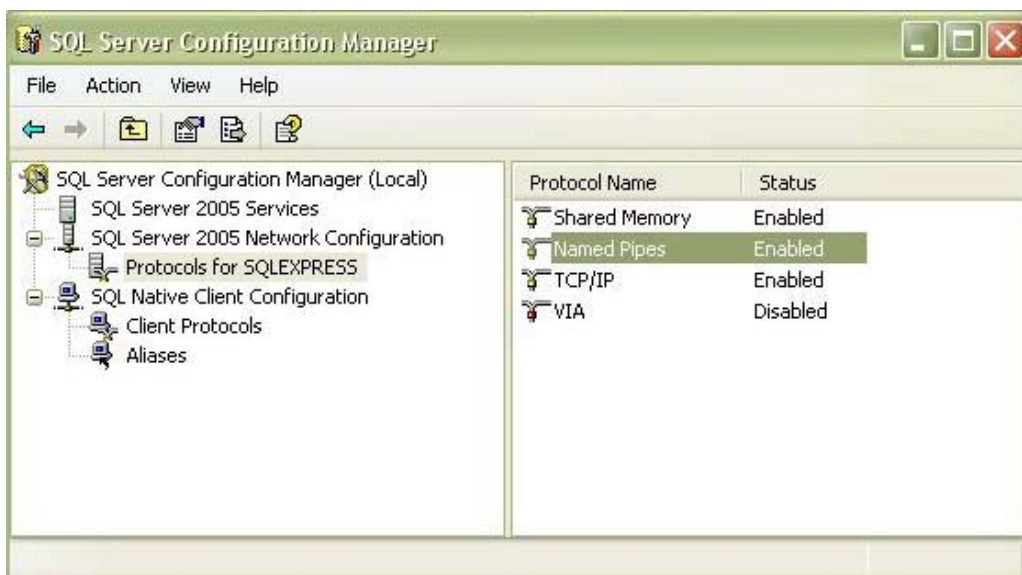
## Other Configurations

### Configuring MSSQL database

NetFlow Analyzer lets users to configure and use MSSQL database.

The steps to configure and run the netflow Analyzer server with SQLSERVER as the database is given below:

1. From the installed MS SQLSERVER, copy the files **bcp.exe** and **bcp.rll** to <NetFlow Analyzer Home>\bin folder.
2. Invoke the <NetFlow Analyzer Home>\bin\changeDBServer.bat, to configure the MS SQLSERVER credentials like ServerName, Port, UserName and Password.
3. **Database Setup Wizard** pops-up.
4. Please check if the TCP/IP ports are turned on. In case they are not, please enable TCP/IP.



5. In the wizard screen, select **Server Type** as **SQL Server**. **Available SQL Server Instances** are listed in a combo box. Enter the **Host Name** and **Port** of the SQL Server from the instances. ( NetFlow Analyzer will work only with default instance)
6. Select the authentication type using the "**Connect Using:**" options.
7. The options are:
  - a. Windows Authentication  
For Windows Authentication, enter the **Domain Name**, **User Name** and **Password**.  
Ensure that both NetFlow Analyzer server and SQL Server are in the same domain and logged in with the same Domain Administrator account.
  - b. SQL Server Authentication  
For SQL Server Authentication, enter the **User Name** and **Password**.
8. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.
9. Click **Save** button to save the SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.
10. Start the netflow Analyzer Server/Service to work with the MS SQLSERVER as the database.

## Migrating NetFlow Analyzer Data from MySQL to MSSQL

## Database

---

NetFlow Analyzer lets users to migrate the existing NetFlow Analyzer data available in MySQL database to MSSQL database.

The steps to migrate and run the NetFlow Analyzer server with SQLSERVER as the database is given below:

1. Stop the NetFlow Analyzer Server/Service.
2. Invoke the `<NetFlow Analyzer Home>\troubleshooting\Mysql_Mssql_BackUpConfig.bat`, to backup the data available in MySQL database and wait till the data backup is getting completed. By default backup file will be stored under `<NetFlow Analyzer Home>\backup` directory with the file name like **'BackupConfig\_NFA\_<Build Number>\_MM\_DD\_YYYY\_hh\_mm.data'**.
3. From the installed MS SQLSERVER, copy the files **bcp.exe** and **bcp.rll** to `<NetFlow Analyzer Home>\bin` folder.
4. Invoke the `<NetFlow Analyzer Home>\bin\changeDBServer.bat`, to configure the MS SQLSERVER credentials like ServerName, Port, UserName and Password.
5. **Database Setup Wizard** pops-up.
6. In the wizard screen, select **Server Type** as *SQL Server*. **Available SQL Server Instances** are listed in a combo box. Enter the **Host Name** and **Port** of the SQL Server from the instances. ( NetFlow Analyzer will work only with default instance)
7. Select the authentication type using the "**Connect Using:**" options.
8. The options are:
  - a. Windows Authentication  
For Windows Authentication, enter the **Domain Name**, **User Name** and **Password**.  
Ensure that both NetFlow Analyzer server and SQL Server are in the same domain and logged in with the same Domain Administrator account.
  - b. SQL Server Authentication  
For SQL Server Authentication, enter the **User Name** and **Password**.
  - c. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.
  - d. Click **Save** button to save the SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.
  - e. Invoke the `<NetFlow Analyzer Home>\bin\run.bat` to start the NetFlow Analyzer server in the command prompt.
  - f. After the server is started completely, stop the server by terminating the **run.bat** in the command prompt or invoke the `<NetFlow Analyzer Home>\bin\shutdown.bat`
  - g. Invoke the `<NetFlow Analyzer Home>\troubleshooting\Mysql_Mssql_RestoreConfig.bat`.
  - h. Start the NetFlow Analyzer server/service.

## **Appendix**

---

1. Working with SSL
2. SNMP Trap Forwarding
3. Database Backup
4. Configuration Backup
5. Aggregated Data Backup
6. Geo Locations

## Working with SSL

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

You can enable secure communication from web clients to the NetFlow Analyzer server using SSL.



The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at <http://www.apache.org> and <http://www.modssl.org>

Stop the server, if it is running, and follow the steps below to enable SSL support:

### Generating a valid certificate

1. Generate the encryption certificate and name it as server.keystore
2. Copy the generated server.keystore file to the `<NetFlowAnalyzer_Home>/server/default/conf` directory

### Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8090). To disable HTTP follow the steps below:

1. Edit the `server.xml` file present in `<NetFlowAnalyzer_Home>/server/default/deploy/jbossweb-tomcat50.sar` directory.
2. Comment out the HTTP connection parameters, by placing the `<!--` tag before, and the `-->` tag after the following lines:

```
<!-- A HTTP/1.1 Connector on port 8090 -->
<Connector port="8090" address="{jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8493" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true" />
```

### Enabling SSL

1. In the same file, enable the HTTPS connection parameters, by removing the `<!--` tag before, and the `-->` tag after the following lines:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore
<Connector port="8493" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

Replace the default values for the following parameters as follows:

Default Value	New Value
keystoreFile=	keystoreFile=
"\${jboss.server.home.dir}/conf/chap8.keystore	"\${jboss.server.home.dir}/conf/server.keystore
keystorePass="rmi+ssl"	keystorePass="pqsecured"

### Changing the web server port

1. Edit the sample-bindings.xml file present in `<NetFlowAnalyzer_Home>/server/default/conf` directory
2. Replace the default values for the following parameters as follows:

Default Value	New Value
<code>&lt;xsl:variable name="portHttps" select="\$port + 363"/&gt;</code>	<code>&lt;xsl:variable name="portHttps" select="8493"/&gt;</code>
<code>&lt;/delegate-config&gt; &lt;binding port="8090"/&gt;</code>	<code>&lt;/delegate-config&gt; &lt;binding port="8493"/&gt;</code>
<code>&lt;/service-config&gt;</code>	<code>&lt;/service-config&gt;</code>

### Verifying SSL Setup

1. Restart the NetFlow Analyzer server
2. Verify that the following message appears:  
Server started.  
Please connect your client at `http://localhost:8493`
3. Connect to the server from a web browser by typing `https://<hostname>:8493` where `<hostname>` is the machine where the server is running

## SNMP Trap Forwarding

---

The alerts generated by Netflow Analyzer can be forwarded as a trap message to any manager application. This helps in consolidating all the network alerts in a single place in the manager application.

The steps for the manager application to get the traps, forwarded by Netflow Analyzer, are;

1. Configure a particular port in the manager application to listen for SNMP traps
2. In Netflow Analyzer alert profile form, select alert action as '**SNMP Trap**' and specify <Server Name>:<Port No.>:<Community>
  - **<Server Name>** - The name or IP address of the server in which the manager application is running
  - **<Port No.>** - The port number at which the manager application is listening for the traps
  - **<Community>** - The community string of the manager application

After the configuration, one trap is sent to the manager application, for every alert generated. A trap contains an OID and a system description.

Entuity provides a MIB file with the OIDs and their descriptions for all the traps that can be forwarded. The manager application can parse this MIB file and get meaningful messages for the forwarded traps.

The steps for the manager application to decode the meaning of each of the OIDs, are;

- Copy ADVENTNET-NETFLOWANALYZER-MIB file from <NetFlow Analyzer Home>/lib directory and save it in the system where the manager application is running
- Load the MIB file, ADVENTNET-NETFLOWANALYZER-MIB in the manager application
- Make the required configuration in the manager application, such that the OIDs are parsed and meaningful info is got

## Database Backup

---

### For MYSQL backup

Please follow the below steps to migrate from one server to another:

1. Shutdown the server.
2. Execute the file *BackupDB.bat/BackupDB.sh* under *<NetFlow\_Home>\troubleshooting* folder. This will create a zip file under *<NetFlow\_Home>* with name *database\_backup\_<build\_number>\_<date>.zip*. ( Please check the zip file to make sure it is not corrupted)
3. Install the NetFlow Analyzer on a new machine and start the server.
4. Shutdown the server.
5. Copy the zip file under *<NetFlow\_home>*, unzip it and restart the server.

### Note:

1. The new server's Operating System must match with that of the old one. Cross platform migration is not supported.
2. The build number of the NetFlow Analyzer should be the same.

### For MSSQL backup

Please get details here -<http://msdn.microsoft.com/en-us/library/ms187048.aspx>

## Configuration Backup

---

Please follow the below steps to take the **backup of configuration data** :

*Step 1:* Shutdown the NetflowAnalyzer server.

*Step 2:* Navigate to <NetFlow\_Home>/troubleshooting folder.

*Step 3:* Run the *backupConfig.bat/backupConfig.sh* file, which will create a *ConfigBackup.sql* under <NetFlow\_Home>

**Note** : The ConfigBackup.sql file will contain all your configuration. Please keep it in a safe location.

Please follow the below steps to **restore the configuration data** :

*Step 1:* Install the NetFlow Analyzer.

*Step 2:* Shutdown the server.

*Step 3:* Copy the *ConfigBackup.sql* under <NetFlow\_Home>

*Step 4:* Navigate to <NetFlow\_Home>/troubleshooting folder.

*Step 5:* Run *restoreConfig.bat / restoreConfig.sh* file.

*Step 6:* Start the server.

## Aggregated Data Backup

---

### For MYSQL backup

Steps to be followed to take backup of the Aggregated data :

1. Shutdown Netflow Analyzer
2. Execute the file **BackupDB.bat -A** ( BackupDB.sh -A, in Case of linux) under \troubleshooting folder. This will create a zip file under <Netflow\_home> with the name **aggregated\_database\_backup.zip** ( Ensure that the zip file is not corrupted )
3. Copy the zip file to a remote backup location
4. Install the Netflow Analyzer (same build)
5. Start Netflow Analyzer
6. Shutdown Netflow Analyzer
7. Copy the zip file under the <Netflow\_home>, and unzip the file at the same location
8. 8.Navigate to the \troubleshooting folder and execute the command **rawCleanup.bat** ( rawCleanup.sh, in Case of Linux)
9. Start the Netflow Analyzer Server

### For MSSQL backup

Please get details here -<http://msdn.microsoft.com/en-us/library/ms187048.aspx>

## Geo Locations

---

Geo Locations is an useful feature which has been added in NetFlow Analyzer "source" and "destination" tab.

Geo locations gives the country wise traffic usage interms of the total volume(in Kbytes) and the total utilization(in %).

To use the "Geo locations" feature, please select the respective interface and click on the source or the destination tab. There you would see "Geo locations" between "Resolve DNS" and "Show network", on the top left.

Click on "Geo locations" and the list of countries with the respective traffic usage will appear. You can click on the country of your choice from the list and view the top ten bandwidth users in terms of their "IP addresses."

You can "Click to update" which is besides "Geo locations" to update the IP locations database. If the IP locations table is up to date then an "IP Locations Database is already up to date" message will pop up. Else the database will be updated.

**NOTE :** When you "click to update" for the first time you might get the following msg "The Geo Location Database file could not be downloaded. Please check whether the proxy settings are correct here. Otherwise please download the file from here and unzip under NetFlow-Home directory"

If so, please **check your proxy settings** and then download again.

At the bottom of the page, a chart which shows the traffic usage of different countries will be displayed. Each country would be displayed according to their traffic usage.